

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-202719

(43)Date of publication of application : 19.07.2002

(51)Int.Cl. G09C 1/00
G06F 12/14

(21)Application number : 2001-066850

(71)Applicant : SONY CORP

(22)Date of filing : 09.03.2001

(72)Inventor : SAKO YOICHIRO
FURUKAWA SHUNSUKE
INOUCHI TATSUYA
KIHARA TAKASHI

(30)Priority

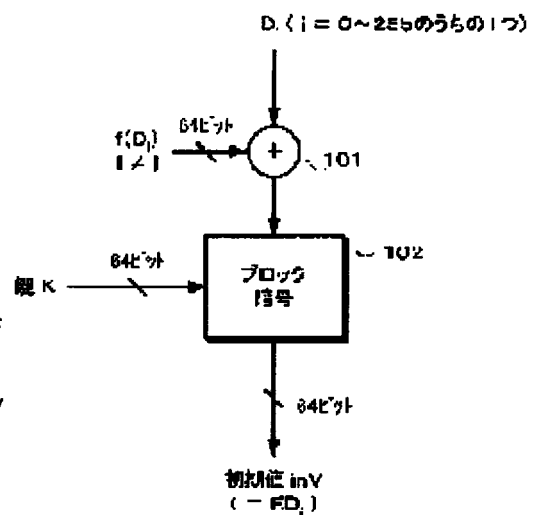
Priority number : 2000337307 Priority date : 06.11.2000 Priority country : JP

(54) DEVICE AND METHOD FOR ENCIPHERING, DEVICE AND METHOD FOR DECIPHERING, AND STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a device and a method for enciphering which enable carrying out of a chain of enciphering without necessitating data or random numbers in a special area for an initial value and have high confidentiality nature, and to provide a device and method for deciphering and a storage medium.

SOLUTION: When data on contents are enciphered and recorded, the data on contents are divided into blocks and the blocks are chained in a chain-like status and enciphered. The initial value at this time is generated from the contents data itself in its sector. In the case of an MPEG stream, the initial value is generated from unique information on a header. Thus, it is not necessary to generate initial value by random numbers, etc., and loss of a data area will not occur. Since the contents data change at random, the confidentiality nature is high. Moreover, the circuit scale can be kept small, because a random number generator and the like is not necessary.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-202719

(P2002-202719A)

(43) 公開日 平成14年7月19日 (2002.7.19)

(51) Int.Cl. ⁷	識別記号	F I	テームコード* (参考)
G 0 9 C 1/00	6 1 0	G 0 9 C 1/00	6 1 0 B 5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B 5 J 1 0 4

審査請求 未請求 請求項の数56 O L (全 26 頁)

(21) 出願番号 特願2001-66850 (P2001-66850)
(22) 出願日 平成13年3月9日 (2001.3.9)
(31) 優先権主張番号 特願2000-337307 (P2000-337307)
(32) 優先日 平成12年11月6日 (2000.11.6)
(33) 優先権主張国 日本 (J P)

(71) 出願人 000002185
ソニー株式会社
東京都品川区北品川6丁目7番35号
(72) 発明者 佐古 曜一郎
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内
(72) 発明者 古川 俊介
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内
(74) 代理人 100082762
弁理士 杉浦 正知

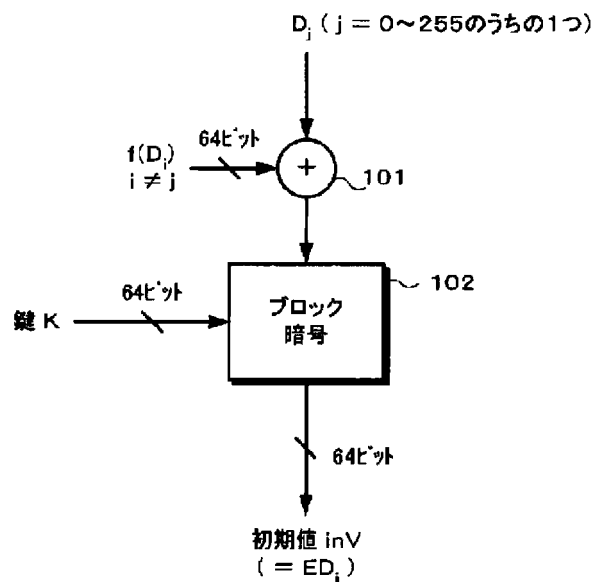
最終頁に続く

(54) 【発明の名称】 暗号化装置及び方法、復号装置及び方法、並びに記憶媒体

(57) 【要約】

【課題】 連鎖的な暗号化を行う場合に、初期値のための特別な領域のデータや乱数が不要であると共に、秘匿性が高くなるようにする。また、データ領域が有効に利用できるようにする。

【解決手段】 コンテンツのデータを暗号化して記録する際に、コンテンツのデータがブロック化され、鎖状に連鎖して暗号化される。このときの初期値は、そのセクタのコンテンツデータそのものから生成される。MPEGストリームの場合には、ヘッダのユニークな情報から生成される。このため、初期値を乱数等で発生させる必要がなく、データ領域のロスがない。また、コンテンツデータはランダムに変化しているため、秘匿性が高い。更に、乱数発生器等を用意する必要がなく、回路規模が増大しない。



【特許請求の範囲】

【請求項 1】 コンテンツデータの第 1 の部分のデータに応じて初期値を生成する生成手段と、

上記生成された初期値に応じて上記コンテンツデータの第 2 の部分のデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、上記コンテンツデータの第 1 及び第 2 の部分のデータとは異なる部分のデータを連鎖的に暗号化する暗号手段とを備えるようにした暗号化装置。

【請求項 2】 更に、上記コンテンツデータを複数ビットからなるブロック単位に分割する分割手段を備え、上記生成手段は、上記分割されたブロック単位で、当該ブロック内の第 1 の部分のデータに応じて初期値を生成するようにした請求項 1 に記載の暗号化装置。

【請求項 3】 上記暗号手段は、上記分割されたブロック単位で、ブロック暗号化方式により暗号化を行うようにした請求項 2 に記載の暗号化装置。

【請求項 4】 上記初期値を暗号化するようにした請求項 1 に記載の暗号化装置。

【請求項 5】 上記コンテンツデータの第 1 の部分のデータを変更可能とした請求項 1 に記載の暗号化装置。

【請求項 6】 コンテンツデータの第 1 の部分のデータに応じて初期値を生成し、上記生成された初期値に応じて上記コンテンツデータの第 2 の部分のデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、上記コンテンツデータの第 1 及び第 2 の部分のデータとは異なる部分のデータを連鎖的に暗号化するようにした暗号化方法。

【請求項 7】 更に、上記コンテンツデータを複数ビットからなるブロック単位に分割し、上記分割されたブロック単位で、当該ブロック内の第 1 の部分のデータに応じて初期値を生成するようにした請求項 6 に記載の暗号化方法。

【請求項 8】 上記分割されたブロック単位で、ブロック暗号化方式により暗号化を行うようにした請求項 7 に記載の暗号化方法。

【請求項 9】 上記初期値を暗号化するようにした請求項 6 に記載の暗号化方法。

【請求項 10】 上記コンテンツデータの第 1 の部分のデータを変更可能とした請求項 6 に記載の暗号化方法。

【請求項 11】 暗号化されたコンテンツデータの第 1 の部分のデータを初期値とし、上記暗号化されたコンテンツデータの第 2 の部分データと上記初期値から上記第 2 の部分を復号化し、当該復号データを出力すると共に、上記第 1 及び第 2 の部分のデータとは異なる部分の暗号化データと、その前の暗号化データとから連鎖的に上記第 1 及び第 2 の部分のデータとは異なる部分を復号化する復号手段と、

上記暗号化されたコンテンツデータの第 1 の部分のデー

タから上記第 1 の部分のデータを生成する生成手段とを備えるようにした復号装置。

【請求項 12】 更に、上記コンテンツデータは、複数ビットからなるブロック単位で暗号化されており、上記復号手段は、上記ブロック単位で、ブロック暗号化方式により復号化を行うようにした請求項 11 に記載の復号装置。

【請求項 13】 上記生成手段は、上記ブロック単位で、上記暗号化されたコンテンツデータの第 1 の部分のデータから上記第 1 の部分のデータを生成するようにした請求項 12 に記載の復号装置。

【請求項 14】 上記初期値は暗号化されており、上記第 1 の部分のデータを上記初期値を復号して生成するようにした請求項 11 に記載の暗号化装置。

【請求項 15】 暗号化されたコンテンツデータの第 1 の部分のデータを初期値とし、上記暗号化されたコンテンツデータの第 2 の部分データと上記初期値から上記第 2 の部分を復号化し、当該復号データを出力すると共に、上記第 1 及び第 2 の部分のデータとは異なる部分の暗号化データと、その前の暗号化データとから連鎖的に上記第 1 及び第 2 の部分のデータとは異なる部分を復号化し、上記暗号化されたコンテンツデータの第 1 の部分のデータから上記第 1 の部分のデータを生成するようにした復号方法。

【請求項 16】 更に、上記コンテンツデータは、複数ビットからなるブロック単位で暗号化されており、上記ブロック単位で、ブロック暗号化方式により復号化を行うようにした請求項 15 に記載の復号方法。

【請求項 17】 上記ブロック単位で、上記暗号化されたコンテンツデータの第 1 の部分のデータから上記第 1 の部分のデータを生成するようにした請求項 16 に記載の復号方法。

【請求項 18】 上記初期値は暗号化されており、上記第 1 の部分のデータを上記初期値を復号して生成するようにした請求項 15 に記載の復号方法。

【請求項 19】 コンテンツデータの第 1 の部分のデータに応じて初期値を生成し、上記生成された初期値に応じて上記コンテンツデータの第 2 の部分のデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、上記コンテンツデータの第 1 及び第 2 の部分のデータとは異なる部分のデータを連鎖的に暗号化して、上記コンテンツのデータを記憶するようにした記憶媒体。

【請求項 20】 コンテンツデータのストリームの所定の部分のデータに応じて初期値を生成する生成手段と、上記生成された初期値に応じて上記コンテンツデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、上記コンテンツデータとは異なる部分のデータを連鎖的に暗号化する暗号手段とを

備えるようにした暗号化装置。

【請求項 2 1】 更に、上記コンテンツデータを複数ビットからなるブロック単位に分割する分割手段を備え、上記暗号手段は、上記分割されたブロック単位で、ブロック暗号化方式により暗号化を行うようにした請求項 2 0 に記載の暗号化装置。

【請求項 2 2】 上記ストリーム中のヘッダの部分に含まれるデータに応じて初期値を生成するようにした請求項 2 0 に記載の暗号化装置。

【請求項 2 3】 上記ストリーム中のヘッダの部分に含まれる時間情報に応じて初期値を生成するようにした請求項 2 0 に記載の暗号化装置。

【請求項 2 4】 上記ストリーム中のヘッダの部分に含まれるコンテンツ毎にユニークな情報に応じて初期値を生成するようにした請求項 2 0 に記載の暗号化装置。

【請求項 2 5】 上記ストリーム中のヘッダの部分に含まれる時間情報と、上記ストリーム中のヘッダの部分に含まれるコンテンツ毎にユニークな情報とに応じて初期値を生成するようにした請求項 2 0 に記載の暗号化装置。

【請求項 2 6】 上記初期値を暗号化するようにした請求項 2 0 に記載の暗号化装置。

【請求項 2 7】 上記ストリームは、MPEG ストリームである請求項 2 0 に記載の暗号化装置。

【請求項 2 8】 上記ヘッダは、バックヘッダ、パケットヘッダ、又はファイルヘッダである請求項 2 7 に記載の暗号化装置。

【請求項 2 9】 コンテンツデータのストリームの所定の部分のデータに応じて初期値を生成し、上記生成された初期値に応じて上記コンテンツデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、上記コンテンツデータとは異なる部分のデータを連鎖的に暗号化するようにした暗号化方法。

【請求項 3 0】 更に、上記コンテンツデータを複数ビットからなるブロック単位に分割し、上記分割されたブロック単位で、ブロック暗号化方式により暗号化を行うようにした請求項 2 9 に記載の暗号化方法。

【請求項 3 1】 上記ストリーム中のヘッダの部分に含まれるデータに応じて初期値を生成するようにした請求項 2 9 に記載の暗号化方法。

【請求項 3 2】 上記ストリーム中のヘッダの部分に含まれる時間情報に応じて初期値を生成するようにした請求項 2 9 に記載の暗号化方法。

【請求項 3 3】 上記ストリーム中のヘッダの部分に含まれるコンテンツ毎にユニークな情報に応じて初期値を生成するようにした請求項 2 9 に記載の暗号化方法。

【請求項 3 4】 上記ストリーム中のヘッダの部分に含まれる時間情報と、上記ストリーム中のヘッダの部分に

含まれるコンテンツ毎にユニークな情報とに応じて初期値を生成するようにした請求項 2 9 に記載の暗号化方法。

【請求項 3 5】 上記初期値を暗号化するようにした請求項 2 9 に記載の暗号化方法。

【請求項 3 6】 上記ストリームは、MPEG ストリームである請求項 2 9 に記載の暗号化方法。

【請求項 3 7】 上記ヘッダは、バックヘッダ、パケットヘッダ、又はファイルヘッダである請求項 3 6 に記載の暗号化方法。

【請求項 3 8】 コンテンツデータのストリームの所定の部分のデータに応じて初期値を生成する生成手段と、暗号化されたコンテンツデータと上記初期値から上記コンテンツデータを復号化し、当該復号データを出力すると共に、暗号化データと、その前の暗号化データとから連鎖的にコンテンツデータを復号化する復号手段とを備えるようにした復号装置。

【請求項 3 9】 更に、上記コンテンツデータは、複数ビットからなるブロック単位で暗号化されており、上記復号手段は、上記ブロック単位で、ブロック暗号化方式により復号化を行うようにした請求項 3 8 に記載の復号装置。

【請求項 4 0】 上記生成手段は、上記ストリーム中のヘッダの部分に含まれるデータに応じて初期値を生成するようにした請求項 3 8 に記載の復号装置。

【請求項 4 1】 上記生成手段は、上記ストリーム中のヘッダの部分に含まれる時間情報に応じて初期値を生成するようにした請求項 3 8 に記載の復号装置。

【請求項 4 2】 上記生成手段は、上記ストリーム中のヘッダの部分に含まれるコンテンツ毎にユニークな情報に応じて初期値を生成するようにした請求項 3 8 に記載の復号装置。

【請求項 4 3】 上記生成手段は、上記ストリーム中のヘッダの部分に含まれる時間情報と、上記ストリーム中のヘッダの部分に含まれるコンテンツ毎にユニークな情報とに応じて初期値を生成するようにした請求項 3 8 に記載の復号装置。

【請求項 4 4】 上記生成手段は、暗号化されている上記初期値を復号化するようにした請求項 3 8 に記載の復号装置。

【請求項 4 5】 上記ストリームは、MPEG ストリームである請求項 3 8 に記載の復号装置。

【請求項 4 6】 上記ヘッダは、バックヘッダ、パケットヘッダ、又はファイルヘッダである請求項 4 5 に記載の復号装置。

【請求項 4 7】 コンテンツデータのストリームの所定の部分のデータに応じて初期値を生成し、暗号化されたコンテンツデータと上記初期値から上記コンテンツデータを復号化し、当該復号データを出力すると共に、暗号化データと、その前の暗号化データとから

連鎖的にコンテンツデータを復号化するようにした復号方法。

【請求項 48】 更に、上記コンテンツデータは、複数ビットからなるブロック単位で暗号化されており、上記復号手段は、上記ブロック単位で、ブロック暗号化方式により復号化を行うようにした請求項 47 に記載の復号装置。

【請求項 49】 上記生成手段は、上記ストリーム中のヘッダの部分に含まれるデータに応じて初期値を生成するようにした請求項 47 に記載の復号装置。

【請求項 50】 上記生成手段は、上記ストリーム中のヘッダの部分に含まれる時間情報に応じて初期値を生成するようにした請求項 47 に記載の復号装置。

【請求項 51】 上記生成手段は、上記ストリーム中のヘッダの部分に含まれるコンテンツ毎にユニークな情報に応じて初期値を生成するようにした請求項 47 に記載の復号装置。

【請求項 52】 上記生成手段は、上記ストリーム中のヘッダの部分に含まれる時間情報と、上記ストリーム中のヘッダの部分に含まれるコンテンツ毎にユニークな情報とに応じて初期値を生成するようにした請求項 47 に記載の復号装置。

【請求項 53】 上記生成手段は、暗号化されている上記初期値を復号化するようにした請求項 47 に記載の復号装置。

【請求項 54】 上記ストリームは、MPEG ストリームである請求項 47 に記載の復号装置。

【請求項 55】 上記ヘッダは、パックヘッダ、パケットヘッダ、又はファイルヘッダである請求項 54 に記載の復号装置。

【請求項 56】 コンテンツデータのストリームの所定の部分のデータに応じて初期値を生成し、上記生成された初期値に応じて上記コンテンツデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、上記コンテンツデータとは異なる部分のデータを連鎖的に暗号化して、上記コンテンツのデータを記憶するようにした記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、例えば CD (Compact Disc) 2 のような光ディスクに、オーディオデータ等のコンテンツのデータを記録／再生する際に、コンテンツのデータの保護を図るためにデータを暗号化して記録するのに用いて好適な暗号化装置及び方法、復号装置及び方法、並びに記憶媒体に関する。

【0002】

【従来の技術】 近年、大容量の記録媒体として光ディスクの開発が進められてきている。例えば音楽情報が記録された CD (Compact Disc)、コンピュータ用のデータが記録される CD-ROM、映像情報を取り扱う DVD (D

igital Versatile Disc または Digital Video Disc) 等が知られている。

【0003】 ここに挙げた光ディスクは、読み出し専用のディスクである。最近では、CD-R (CD-Recordable) ディスク、CD-RW (CD-Rewritable) ディスク等のように、データの追記や、書き換えが可能な光ディスクが実用化されている。さらに、CD と同様な形状で記録容量を高めた倍密度 CD や、通常の CD プレーヤとパーソナルコンピュータとの双方との親和性が高められる CD 2 等、様々な光ディスクの開発が進められている。

【0004】 このような光ディスクの普及に伴って、光ディスクに記録されたコンテンツのデータが不正に複製されて使用されたり、複製されたものが不正に販売されたりして、著作権者に不利益を与えることが危惧されている。そこで、光ディスクにオーディオデータやビデオデータのようなコンテンツデータを記録する際に、著作権者の権利を保護することを目的として、コンテンツデータに対して暗号化処理を施すことが行われている。

【0005】 このように、光ディスクにコンテンツのデータを記録する際に用いる暗号化方式としては、DES (Data Encryption Standard) や tripple DES 等のブロック暗号が使われてきている。DES は代表的な共通鍵暗号であり、64 ビット (8 バイト) のデータを初期転置 (スクランブル) を行い、32 ビットずつ分けたデータを、56 ビットの 1 個の暗号鍵から生成された 16 個の鍵で次々と非線形処理を行い、再び転置を行って、暗号化するものである。

【0006】 ところが、DES のようなブロック暗号は、ブロックの長さが比較的短いため、類似のブロックが頻繁に現れる可能性があり、暗号強度に問題がある。

【0007】 そこで、暗号強度を上げるために、CBC (Ciphering Block Chaining) 方式を用いることが考えられている。CBC 方式は、ブロック単位で暗号化したデータを連鎖させていくことで暗号強度を上げていくものである。

【0008】 すなわち、CBC 方式では、暗号化を行う際には、今回の入力ブロックデータと、その 1 つ前のブロックデータを暗号化したデータとの EX-OR がとられ、暗号化される。復号化を行う際には、暗号化ブロックデータが復号化され、その前の暗号化ブロックデータとの EX-OR がとられて、元のブロックデータが復号される。このように、CBC 方式では、前のブロックデータと連鎖させながら暗号化されるため、暗号強度を上げることができる。

【0009】

【発明が解決しようとする課題】 このように、光ディスクにコンテンツのデータを記録する際に、CBC 方式で暗号化を行うと、暗号強度が上げられ、より、強力に、著作権の保護を図ることができる。ところが、CBC 方式では、前のブロックデータと連鎖させながら暗号化し

ていくため、暗号化を行う際の最初のブロックでは、直前の暗号化ブロックがないため、初期値を用意する必要がある。このように CBC 方式で暗号化を行う際の初期値としては、固定値を使うことが最も簡単である。ところが、CBC 方式の暗号化を行う際の初期値として固定値を用いたのでは、秘匿性に問題があり、高い暗号強度が維持できない。また、初期値として固定値を用意するためには、この初期値となる固定値をどこかにストアしておく必要が生じる。

【0010】そこで、暗号化のブロックには含まれていない他の領域のデータから初期値を作ることが考えられる。例えば、エラー訂正のための ECC (Error Correcting Code) や媒体情報が含まれている。これらのデータは、著作権を有するようなデータそのものではないので、保護する必要はなく、通常、暗号化のブロックには含められない。そこで、ECC や媒体情報のような、他の領域のデータから初期値を作ることが考えられる。

【0011】つまり、図 25 は、ECC や媒体情報のような他の領域のデータから、CBC 方式で暗号化を行う際の初期値を作るようにした例である。図 25 に示すように、入力ブロックデータ D_i を 0 ~ 255 までの 256 個のブロックデータとし、1 ブロックは 8 バイト (64 ビット) とする。

【0012】最初に、初期値 inV として、他の領域からのデータが入力され、EX-OR ゲート 501 で、入力ブロックデータ D_0 と初期値 inV との EX-OR がとられ、これがブロック暗号化回路 502 で鍵情報 K により暗号化されて、暗号化ブロックデータ ED_0 が生成される。

【0013】次に、EX-OR ゲート 501 で、入力ブロックデータ D_1 と、その前の暗号化ブロックデータ ED_0 との EX-OR がとられ、これがブロック暗号化回路 102 で鍵情報 K により暗号化されて、暗号化ブロックデータ ED_1 が生成される。

【0014】以下、入力ブロックデータ D_i と、その前の暗号化ブロックデータ ED_{i-1} との EX-OR がとられ、これがブロック暗号化回路 502 で鍵情報 K により暗号化されて、暗号化ブロックデータ ED_i が生成される。

【0015】このように、初期値 inV をブロックのデータ以外、例えば、ECC や媒体情報から作るようにすれば、初期値が固定値とならないため、秘匿性が上がる。

【0016】ところが、このように、初期値 inV をブロックのデータ以外、例えば、ECC や媒体情報から作るようにすると、コンテンツデータ以外のデータが暗号化のために必ず必要になる。このため、コンテンツデータのみを暗号化してデータ伝送することができなくなり、コンテンツのデータを伝送する際には、必ず、ECC や媒体情報を一緒に送る必要が生じてくる。

【0017】また、CBC 方式で暗号化を行う際の初期値を発生するための他の方法として、初期値を乱数により発生させることが考えられる。

【0018】つまり、図 26 に示すように、最初に、乱数により発生された値が初期値としてブロックデータ D_0 に入れられる。

【0019】この初期値の入ったブロックデータ D_0 は、ブロック暗号化回路 512 で鍵情報 K により暗号化されて、暗号化ブロックデータ ED_1 が生成される。

【0020】次に、EX-OR ゲート 511 で、入力ブロックデータ D_1 と、その前の暗号化ブロックデータ ED_0 との EX-OR がとられ、これがブロック暗号化回路 512 で鍵情報 K により暗号化されて、暗号化ブロックデータ ED_1 が生成される。

【0021】以下、入力ブロックデータ D_i と、その前の暗号化ブロックデータ ED_{i-1} との EX-OR がとられ、これがブロック暗号化回路 512 で鍵情報 K により暗号化されて、暗号化ブロックデータ ED_i が生成される。

【0022】しかしながら、このように、乱数により初期値を発生させると、ブロックデータ D_0 には乱数により発生された初期値が入ることになり、ブロックデータ D_0 には、コンテンツデータが入れられなくなる。したがって、1 セクタの 0 ~ 255 までの 256 ブロック (2048 バイト) のうちの 2040 バイトにしかコンテンツデータを入れることができなくなり、データ領域が有効に利用できないという問題が生じてくる。

【0023】また、初期値を乱数により発生させるようにするためには、乱数発生回路が必要になる。秘匿性を高めるためには、乱数としてランダムな符号を発生できるものが必要であり、このような乱数発生回路を設けると、回路規模が増大するという問題が生じてくる。

【0024】したがって、この発明の目的は、連鎖的な暗号化を行う場合に、初期値のための特別な領域のデータや乱数が不要であり、しかも、秘匿性が高い暗号化装置及び方法、復号装置及び方法、並びに記憶媒体を提供することにある。

【0025】この発明の他の目的は、連鎖的な暗号化を行う場合に、データ領域が有効に利用できる暗号化装置及び方法、復号装置及び方法、並びに記憶媒体を提供することにある。

【0026】

【課題を解決するための手段】請求項 1 の発明は、コンテンツデータの第 1 の部分のデータに応じて初期値を生成する生成手段と、生成された初期値に応じてコンテンツデータの第 2 の部分のデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、コンテンツデータの第 1 及び第 2 の部分のデータとは異なる部分のデータを連鎖的に暗号化する暗号手段とを備えるようにした暗号化装置である。

【0027】請求項6の発明は、コンテンツデータの第1の部分のデータに応じて初期値を生成し、生成された初期値に応じてコンテンツデータの第2の部分のデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、コンテンツデータの第1及び第2の部分のデータとは異なる部分のデータを連鎖的に暗号化するようにした暗号化方法である。

【0028】請求項11の発明は、暗号化されたコンテンツデータの第1の部分のデータを初期値とし、暗号化されたコンテンツデータの第2の部分データと初期値から第2の部分を復号化し、当該復号データを出力すると共に、第1及び第2の部分のデータとは異なる部分の暗号化データと、その前の暗号化データとから連鎖的に第1及び第2の部分のデータとは異なる部分を復号化する復号手段と、暗号化されたコンテンツデータの第1の部分のデータから第1の部分のデータを生成する生成手段とを備えるようにした復号装置である。

【0029】請求項15の発明は、暗号化されたコンテンツデータの第1の部分のデータを初期値とし、暗号化されたコンテンツデータの第2の部分データと初期値から第2の部分を復号化し、当該復号データを出力すると共に、第1及び第2の部分のデータとは異なる部分の暗号化データと、その前の暗号化データとから連鎖的に第1及び第2の部分のデータとは異なる部分を復号化し、暗号化されたコンテンツデータの第1の部分のデータから第1の部分のデータを生成するようにした復号方法である。

【0030】請求項19の発明は、コンテンツデータの第1の部分のデータに応じて初期値を生成し、生成された初期値に応じてコンテンツデータの第2の部分のデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、コンテンツデータの第1及び第2の部分のデータとは異なる部分のデータを連鎖的に暗号化して、コンテンツのデータを記憶するようにした記憶媒体である。

【0031】請求項20の発明は、コンテンツデータのストリームの所定の部分のデータに応じて初期値を生成する生成手段と、生成された初期値に応じてコンテンツデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、コンテンツデータとは異なる部分のデータを連鎖的に暗号化する暗号手段とを備えるようにした暗号化装置である。

【0032】請求項29の発明は、コンテンツデータのストリームの所定の部分のデータに応じて初期値を生成し、生成された初期値に応じてコンテンツデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、コンテンツデータとは異なる部分のデータを連鎖的に暗号化するようにした暗号化方法である。

【0033】請求項38の発明は、コンテンツデータの

ストリームの所定の部分のデータに応じて初期値を生成する生成手段と、暗号化されたコンテンツデータと初期値からコンテンツデータを復号化し、当該復号データを出力すると共に、暗号化データと、その前の暗号化データとから連鎖的にコンテンツデータを復号化する復号手段とを備えるようにした復号装置である。

【0034】請求項47の発明は、コンテンツデータのストリームの所定の部分のデータに応じて初期値を生成し、暗号化されたコンテンツデータと初期値からコンテンツデータを復号化し、当該復号データを出力すると共に、暗号化データと、その前の暗号化データとから連鎖的にコンテンツデータを復号化するようにした復号方法である。

【0035】請求項56の発明は、コンテンツデータのストリームの所定の部分のデータに応じて初期値を生成し、生成された初期値に応じてコンテンツデータを暗号化し、暗号化データを出力すると共に、当該出力される暗号化データに応じて、コンテンツデータとは異なる部分のデータを連鎖的に暗号化して、コンテンツのデータを記憶するようにした記憶媒体である。

【0036】コンテンツのデータがブロック化され、鎖状に連鎖して暗号化される。そして、このときの初期値を、そのセクタのコンテンツデータそのものから生成している。このため、初期値を乱数等で発生する必要がなく、データ領域のロスがない。また、コンテンツデータはランダムに変化しているため、秘匿性が高い。更に、乱数発生器等を容易する必要がなく、回路規模が増大しない。

【0037】また、コンテンツデータから生成される初期値自体が他のコンテンツデータで暗号化される。更に、初期値として使うコンテンツデータを自由に選ぶことができる。これにより、秘匿性が向上される。

【0038】さらに、MPEGストリームを記録する場合には、ヘッダに含まれるユニークな情報を使って、初期値を生成している。ヘッダの情報はユニークであり、SCRやPTSのような時間情報は、時間と共に変化するため、秘匿性が高い。また、MPEGストリームのヘッダの情報を使って暗号化の初期値を形成しているので、MPEGストリームを保ったまま、伝送することができる。さらに、乱数発生器等を容易する必要がなく、回路規模が増大しない。

【0039】

【発明の実施の形態】以下、この発明の実施の形態について図面を参照して説明する。この発明は、例えば、CD (Compact Disc) 2にコンテンツデータを記録／再生する際に、データの保護を図るために、コンテンツのデータを暗号化するのに用いて好適である。

【0040】図1は、この発明が適用できるCD2の外観の構成を示すものである。CD2は、通常のCDと同様に、例えば直径120mmの光ディスクである。ただ

し、所謂シングルCDのように、直径80mmとしても良い。

【0041】CD2は、既存のCDプレーヤと、パーソナルコンピュータとの双方との親和性を考慮して開発されている。このようなCD2は、図1に示すように、その中心にセンターホールが設けられ、内周側に領域AR1が設けられ、さらにその外周に、領域AR2が設けられる。内周側の領域AR1と、外周側の領域AR2との間には、ミラー部M1が設けられ、このミラー部M1により、内周側の領域AR1と外周側の領域AR2とが区切られている。内周側の領域AR1の最内周には、リードイン領域LIN1が設けられ、その最外周には、リードアウト領域LOUT1が設けられる。外周側の領域AR2の最内周には、リードイン領域LIN2が設けられ、その最外周には、リードアウト領域LOUT2が設けられる。

【0042】内周側の領域AR1は、既存のCDプレーヤとの親和性が図られた領域である。この領域AR1には、通常のCDプレーヤでも再生できるように、例えば、オーディオデータが通常のCD-DA (CD Digital Audio) と同様なフォーマットで記録されている。また、この内周側の領域AR1は、通常のCD-DAと同様に扱えるように、通常、コンテンツのデータに対する暗号化は行われない。勿論、著作権の保護を図るために、この内周側の領域AR1に記録するデータを暗号化する場合も考えられる。また、この内周側の領域AR1に、ビデオデータや、コンピュータプログラムデータ等、オーディオデータ以外のデータを記録するようにしても良い。また、この内周側の領域AR1に、コンテンツのデータを圧縮して記録するようにしても良い

【0043】これに対して、外周側の領域AR2は、パーソナルコンピュータとの親和性を図るようにした領域である。この領域AR2には、倍密度でデータが記録できる。この領域AR2には、例えば、オーディオデータが圧縮されて記録される。圧縮方式としては、例えばMP3 (Mpeg-1 Audio Layer-3) 方式が用いられており、また、パーソナルコンピュータとの親和性が図れるように、ファイル化されている。

【0044】MP3は、MPEG1で規定されている3つのレイヤの圧縮方式の1つであり、各帯域の出力をMDCT (Modified Cosine Transform) で周波数軸に分割し、量子化した後、ハフマン符号化するようにしたものである。オーディオデータをMP3方式で圧縮することで、記録容量を拡大できると共に、パーソナルコンピュータと同様のファイルシステムでデータを扱うことができる。このため、外周側の領域AR2にMP3方式でファイル化されて記録されているコンテンツのデータを、パーソナルコンピュータのハードディスクに移動させて、パーソナルコンピュータに音楽サーバを構築したり、フラッシュメモリが装着される携帯型のMP3再生

プレーヤに移動させて、外で音楽再生を楽しんだりすることが容易になる。

【0045】このように、外周側の領域AR2に記録されているコンテンツのデータは、パーソナルコンピュータとの親和性が図られ、取り扱いが容易である。ところが、この外周側の領域AR2に記録されているコンテンツのデータは、外部に持ち出されることが多くなるため、著作権の保護が守られなくなる可能性が高い。このため、外周側の領域AR2に記録されるコンテンツのデータには、コピーや再生を制限するために、暗号化処理が施されるとともに、この外周側の領域AR2には、例えば、コピー禁止/許可、コピーの世代管理、コピーの個数制限、再生禁止/許可、再生回数の制限、再生時間の制限等を管理するための著作権管理情報が記録される。

【0046】なお、ここでは、領域AR2に記録するデータをMP3でファイル化しているが、勿論、領域AR2に記録されるコンテンツのデータは、MP3のファイルに限られるものではない。オーディオデータの圧縮方式としては、MP3の他に、MPEG2-AAC (Advanced Audio Coding)、ATRAC3等が知られている。また、オーディオデータに限らず、ビデオデータや静止画データ、テキストデータ、コンピュータプログラム等、様々なデータを領域AR2に記録することが可能である。また、領域AR2に記録するコンテンツのデータであっても、暗号化する必要がなければ、暗号化せずに記録しても良い、

【0047】このように、CD2は、内周側の領域AR1を使って、通常のCDと同様にCDプレーヤで再生することができ、外周側の領域AR2を使うことで、パーソナルコンピュータや携帯型のプレーヤと連携させながら、データ扱うことができる。

【0048】この発明は、このようなCD2において、特に、外周側の領域AR2に、コンテンツのデータを暗号化して記録/再生するのに用いて好適である。

【0049】図2は、この発明が適用された記録装置の一例である。図2において、入力端子1にコンテンツデータが供給される。コンテンツデータは、例えば、オーディオデータである。オーディオデータとしては、PCMデータでも良いし、MP3等のストリームであっても良い。また、オーディオデータの他、動画データ、静止画データ、ゲームのプログラムデータ、ウェブページのデータ、テキスト等、種々のものをコンテンツデータとして記録することが考えられる。この入力端子1からのコンテンツデータは、暗号化回路4に供給される。

【0050】また、入力端子2に鍵情報Kが供給される。入力端子2からの鍵情報Kが暗号化回路4に供給される。

【0051】暗号化回路4は、入力端子1からのコンテンツデータを、入力端子2からの鍵情報Kを用いて暗号

化するものである。暗号化方式としては、ブロック暗号が用いられる。ブロック暗号は、例えば、8バイトずつを単位として暗号化を行っており、暗号化回路4はブロック化回路を備えている。この例では、ブロック単位で暗号化したデータを連鎖させていくことで、暗号化強度を上げるようにしている。このように、ブロック単位で暗号化したデータを連鎖させていくようなものは、CBC (Ciphering Block Chaining) 方式として知られている。

【0052】暗号化回路4の出力がエラー訂正符号化回路5に供給される。エラー訂正符号化回路5で、暗号化回路4で暗号化されたコンテンツデータに対して、エラー訂正符号が付加される。

【0053】エラー訂正符号化回路5の出力は、変調回路6に供給される。変調回路6で、記録データが所定の変調方式で変調される。変調回路6の出力が記録回路7に供給される。

【0054】記録回路7の出力が光学ピックアップ8に供給される。記録回路7は、システムコントローラ13により制御される。光学ピックアップ8により、光ディスク10に、データが記録される。光ディスク10は、例えば、CD2の光ディスクである。

【0055】光学ピックアップ8は、光ディスク10の半径方向に移動可能とされている。また、図示していないが、光学ピックアップ8からのレーザー光を光ディスク10のトラックに沿って照射するためのトラッキングサーボ回路や、光学ピックアップ8からのレーザー光のスポットを光ディスク10上に合焦させるためのフォーカスサーボ回路、光ディスク10の回転を制御するスピンドルサーボ回路等、各種のサーボ回路が設けられている。

【0056】また、入力端子2からの鍵情報Kがミックス回路9に供給される。入力端子3に著作権管理情報Rが供給され、この著作権管理情報Rが書き換え回路11を介して、ミックス回路9に供給される。ミックス回路9の出力が記録回路12を介して光学ピックアップ8に供給される。光学ピックアップ8により、記録回路12により、光ディスク10に鍵情報Kや著作権管理情報Rが記録される。

【0057】著作権管理情報Rは、例えば、コピー禁止/許可、コピーの世代管理、コピーの個数制限、再生禁止/許可、再生回数の制限、再生時間の制限等を管理するための情報である。コピーの世代管理やコピーの個数制限、再生回数の制限や再生時間の制限を行う場合には、コピーや再生が行われる毎に、著作権管理情報Rを書き換える必要がある。この著作権管理情報Rの書き換えは、書き換え回路11により行われる。

【0058】また、鍵情報Kや著作権管理情報Rの記録場所については、光ディスク10のリードインやリードアウト領域に記録したり、トラックの半径方向にウォブ

ルデータとして記録したりすることが考えられる。

【0059】図3は、再生系の構成を示すものである。図3において、光ディスク20の記録信号は、光学ピックアップ22で再生される。光ディスク20は、図2における光ディスク10と対応しており、光ディスク20としては、例えば、CD2が用いられる。光学ピックアップ22の出力が再生アンプ23を介して、復調回路24に供給される。光学ピックアップ22の動きは、システムコントローラ29の制御の基に、アクセス制御回路30により制御される。アクセス制御回路30は、光学ピックアップの送り機構、光学ピックアップ22からのレーザー光を光ディスク20のトラックに沿って照射するためのトラッキングサーボ回路や、光学ピックアップ22からのレーザー光のスポットを光ディスク20上に合焦させるためのフォーカスサーボ回路等のサーボ回路からなる。

【0060】復調回路24の出力がエラー訂正回路25に供給される。エラー訂正回路25で、エラー訂正処理がなされる。エラー訂正回路25の出力が暗号解読回路26に供給されると共に、鍵管理情報読出回路27に供給される。鍵管理情報読出回路27の出力が暗号解読回路26に供給される。

【0061】暗号解読回路26は、鍵管理情報読出回路27で読み出された鍵情報Kを使って、再生データの暗号解読の処理を行うものである。前述したように、この例では、暗号化方式として、CBC方式が使われている。暗号解読回路26は、このようなCBC方式の暗号の解読処理を行うものである。

【0062】暗号解読回路26の出力が再生回路28に供給される。再生回路28の出力が出力端子31から出力される。また、鍵管理情報読出回路27で読み出された著作権管理情報Rにより、コピーや再生が制限される。

【0063】上述のように、この例では、暗号化方式として、CBC方式が使われている。すなわち、記録系においては、暗号化回路4で、入力されたコンテンツデータに対して、CBC方式により、暗号化処理が行われる。そして、再生系においては、暗号解読回路26により、再生されたコンテンツデータに対して、暗号解読処理が行われる。

【0064】なお、ブロック暗号は、DESやAES、FEAL、MISTY等、何を用いても良い。

【0065】CBC方式では、ブロック単位で暗号化したデータを連鎖させることで、暗号の強度が上げられる。この例では、図4に示すように、2048バイトが1セクタとされ、このセクタを単位として、光ディスク10、20へのデータの記録/再生が行われる。

【0066】つまり、CDでは、98フレームからなるサブコードブロックが1セクタとされている。この1セクタの領域の大きさは2352バイトであり、そのう

ち、2048バイトがデータ領域となっている。

【0067】例えば、DES方式で暗号化する場合に
は、64ビットを1ブロックとして処理され、56ビ
ットの鍵が用いられる。このため、図5に示すように、1
セクタは、8バイト（64ビット）単位で、256のブ
ロックに分割される。

【0068】そして、各セクタ内において、前ブロック
と連鎖させながら、CBC方式により、暗号化処理が行
われる。

【0069】すなわち、CBC方式では、今回のブロッ
クデータと、その1つ前のブロックデータを暗号化した
データとのEX-ORがとられ、これが暗号化される。
1つのセクタ内でCBC方式により暗号化処理が終了し
たら、次のセクタで、また、同様に、CBC方式により
暗号化処理が行われる。

【0070】このように、この例では、CBC方式を用
いることにより、暗号の強度が上げられる。そして、各
セクタでCBC方式で暗号化が行われている。このた
め、エラーの発生等によりデータの再生が不可能になっ
たような場合でも、その影響がそのセクタ内で完結し、
他のセクタにおよぶことがなくなる。

【0071】そして、この発明の実施の形態では、初期
値として、同一セクタ内のブロックのデータが利用され
る。このように、同一のセクタ内のブロックのデータを
初期値として使うことで、データ領域のロスがなくな
る。また、音楽データや画像データのようなコンテンツ
データの場合には、それ自体の値がランダムに変化して
いる。このため、コンテンツのデータを利用すると、初
期値の秘匿性も高い。

【0072】初期値として同一セクタ内のブロックのデ
ータを利用する場合、そのデータそのものでは、秘匿性
が十分でない。そこで、同一のセクタ内のブロックのデ
ータを暗号化したものを初期値として利用することが考
えられる。更に、この例では、同一セクタ内の1つのブ
ロックデータと、そのセクタ内のそれ以外のブロックデ
ータとのEX-ORをとり、これを暗号化したものを初
期値としている。

【0073】つまり、図6及び図7を使って、暗号化処
理について説明する。図6は、初期値を生成するときの
プロセスを示し、図7は、連鎖的にブロック暗号を行う
ときのプロセスを示すものである。

【0074】暗号化処理を行う場合には、先ず、図6に
示すようにして、初期値が生成される。

【0075】すなわち、図6に示すように、D0～D25
5までの1セクタ内のブロックデータのうちの1つD_j
がEX-ORゲート101に送られる。また、同一のセ
クタ内のブロックデータD_jを除くブロックデータD_i
の関数f(D_i)がEX-ORゲート101に送られ
る。

【0076】EX-ORゲート101で、ブロックデー

タD_jと、ブロックデータD_j以外のブロックデータD_i
の関数f(D_i)とのEX-ORが求められる。

【0077】なお、ブロックデータD_jと、ブロックデ
ータD_j以外の全てのブロックデータD_iの関数f(D_i)
とのEX-ORは、ブロックデータD_jと、ブロッ
クデータD_j以外の全てのブロックデータD_iの関数f
(D_i)とのEX-ORでも良いし、ブロックデータD_j
と、ブロックデータD_j以外の1つのブロックデータ
D_iの関数f(D_i)とのEX-ORでも良いし、ブロッ
クデータD_iの数をいくつにしても良い。また、関数
f(D_i)も、何を用いても良い。

【0078】このEX-ORゲート101の出力は、ブ
ロック暗号化回路102に送られる。ブロック暗号化回
路102で、EX-ORゲート101の出力が鍵情報K
により暗号化される。これにより、初期値i_nVが求め
られる。また、この値は、ブロックデータD_jを暗号化
したデータED_jとしても用いられる。

【0079】このようにして、初期値が求められたら、
図7に示すように、この初期値を使って、今回のブロッ
クデータと、その1つ前のブロックデータを暗号化した
データとのEX-ORがとられ、これが暗号化される。
そして、ブロックデータD_jのときには、初期値として
も使われているデータED_jが暗号化したブロックデー
タとして使われる。

【0080】つまり、初期値として使った入力ブロック
データD_jが(j=1～254)の何れかであるときには
は、以下のようにして暗号化が行われる。

【0081】先ず、EX-ORゲート111で、入力ブ
ロックデータD0と、図6で求められた初期値i_nVと
のEX-ORがとられ、このEX-ORゲート111の
出力がブロック暗号化回路112に供給される。

【0082】ブロック暗号化回路112で、EX-OR
ゲート111の出力と鍵情報Kとから、暗号化ブロック
データED0が求められる。

【0083】次に、EX-ORゲート111で、入力ブ
ロックデータD1と、暗号化ブロックデータED0との
EX-ORがとられ、このEX-ORゲート111の出
力がブロック暗号化回路112に供給され、ブロック暗
号化回路112で、EX-ORゲート111の出力と鍵
情報Kとから、暗号化ブロックデータED1が求められ
る。

【0084】以下、同様にして、入力データD2、D3
、…から、暗号化ブロックデータED2、ED3、…
が求められる。

【0085】入力ブロックデータD2、D3、…を暗号
化していき、入力ブロックデータがD_jになったら、図
6で求められた初期値i_nVが暗号化ブロックデータE
D_jとして出力される。

【0086】そして、再び、EX-ORゲート111
で、入力ブロックデータD_iと、暗号化ブロックデータ

ED_{i-1} との EX-OR がとられ、この EX-OR ゲート 111 の出力がブロック暗号化回路 112 に供給され、ブロック暗号化回路 112 で、EX-OR ゲート 111 の出力と鍵情報 K とから、暗号化ブロックデータ ED_i が求められる。

【0087】入力データ D255 が暗号化されて暗号化ブロックデータ ED255 が出力されるまで、同様の処理が繰り返される。

【0088】初期値として使った入力ブロックデータ D_j が最初のブロックデータ (j=0) のときには、以下のようにして暗号化が行われる。

【0089】まず、図 6 で求められた初期値 i n V が暗号化ブロックデータ ED0 として出力される。

【0090】それから、図 7 に示す EX-OR ゲート 111 で、入力ブロックデータ D1 と、暗号化ブロックデータ ED0 (初期値 i n V と等しい) との EX-OR ゲートがとられ、この EX-OR ゲート 111 の出力がブロック暗号化回路 112 に供給され、ブロック暗号化回路 112 で、EX-OR ゲート 111 の出力と鍵情報 K とから、暗号化ブロックデータ ED1 が求められる。

【0091】以下、入力データ D255 が暗号化されて暗号化ブロックデータ ED255 が出力されるまで、同様の処理が繰り返され、入力データ D2、D3、…から、暗号化ブロックデータ ED2、ED3、…が求められる。

【0092】初期値として使った入力ブロックデータ D_j が最後のブロックデータ (j=255) のときには、以下のようにして暗号化が行われる。

【0093】まず、図 7 に示す EX-OR ゲート 111 で、入力ブロックデータ D0 と、図 6 で求められた初期値 i n V との EX-OR がとられ、この EX-OR ゲート 111 の出力がブロック暗号化回路 112 に供給される。

【0094】ブロック暗号化回路 112 で、EX-OR ゲート 111 の出力と鍵情報 K とから、暗号化ブロックデータ ED0 が求められる。

【0095】次に、EX-OR ゲート 111 で、入力ブロックデータ D1 と、暗号化ブロックデータ ED0 との EX-OR がとられ、この EX-OR ゲート 111 の出力がブロック暗号化回路 112 に供給され、ブロック暗号化回路 112 で、EX-OR ゲート 111 の出力と鍵情報 K とから、暗号化ブロックデータ ED1 が求められる。

【0096】以下、同様に、入力データ D2、D3、…から、暗号化ブロックデータ ED2、ED3、…が求められる。入力データ D254 の暗号化ブロックデータ ED254 が求められるまで、同様の処理が繰り返される。

【0097】最後のブロックデータ D255 になったら、図 6 で求められた初期値 i n V が暗号化ブロックデータ ED255 として出力される。

【0098】次に、図 8 及び図 9 を使って、復号化処理について説明する。図 8 は、連鎖的にブロック暗号を行うときのプロセスを示すものであり、図 9 は、初期値を暗号化したブロックデータを復号するときのプロセスを示すものである。

【0099】初期値として使った入力ブロックデータ D_j が (j=1~254) の何れかであるときには、以下のようにして復号化が行われる。

【0100】まず、図 8 に示すように、暗号化ブロックデータ ED0 と、鍵情報 K とがブロック暗号復号回路 121 に送られ、ブロック暗号復号回路 121 で、暗号の復号処理が行われる。

【0101】ブロック暗号復号回路 121 の出力が EX-OR ゲート 122 に送られる。また、EX-OR ゲート 122 には、初期値 i n V が送られる。この初期値 i n V は、暗号化ブロックデータ ED_j である。

【0102】EX-OR ゲート 122 で、ブロック暗号復号回路 121 の出力と、暗号化ブロックデータ ED_j との EX-OR がとられて、ブロックデータ D0 が復号される。

【0103】次に、暗号化ブロックデータ ED1 と、鍵情報 K とがブロック暗号復号回路 121 に送られる。ブロック暗号復号回路 121 で暗号が復号される。ブロック暗号復号回路 121 の出力が EX-OR ゲート 122 に送られる。

【0104】また、EX-OR ゲート 122 には、その前の暗号化ブロックデータ ED0 とが送られる。

【0105】EX-OR ゲート 122 で、ブロック暗号復号回路 121 の出力と、その前の暗号化ブロックデータ ED0 との EX-OR がとられて、ブロックデータ D1 が復号される。

【0106】以下、同様に、暗号化ブロックデータ ED1、ED2、…から、ブロックデータ D1、D2、…が復号されていく。

【0107】このように、ブロックデータ D2、D3、…を復号化していく間に、復号するブロックデータが初期値に相当する暗号化ブロックデータ ED_j になったら、図 9 に示すように、暗号化ブロックデータ ED_j と、鍵情報 K とがブロック暗号復号回路 131 に送られ、ブロック暗号復号回路 131 で暗号の復号処理が行われる。

【0108】ブロック暗号復号回路 131 の出力が EX-OR ゲート 132 に送られる。また、EX-OR ゲート 132 には、ブロックデータ D_j 以外のデータとの間の関数 f (D_i) が送られる。

【0109】EX-OR ゲート 132 で、ブロック暗号復号回路 131 の出力と、ブロックデータ D_j 以外のデータとの間の関数 f (D_i) との EX-OR がとられて、ブロックデータ D_j が復号される。

【0110】ブロックデータ D_j が復号されたら、図 8

に戻り、暗号化ブロックデータ ED_i と、鍵情報 K とがブロック暗号復号回路 121 に送られる。ブロック暗号復号回路 121 で暗号が復号される。ブロック暗号復号回路 121 の出力が EX-OR ゲート 122 に送られる。また、EX-OR ゲート 122 には、その前の暗号化ブロックデータ ED_{i-1} が送られる。EX-OR ゲート 122 で、ブロック暗号復号回路 121 の出力と、その前の暗号化ブロックデータ ED_{i-1} との EX-OR がとられて、ブロックデータ D_i が復号される。

【0111】以下、暗号化ブロックデータ ED_{255} が復号されるまで、同様な処理が繰り返される。

【0112】初期値として使った入力ブロックデータ D_j が最初のブロックデータ ($j=0$) のときには、以下のようにして復号化が行われる。

【0113】まず、図 9 に示すように、暗号化ブロックデータ ED_0 と、鍵情報 K とがブロック暗号復号回路 131 に送られ、ブロック暗号復号回路 131 で暗号の復号処理が行われる。

【0114】ブロック暗号復号回路 131 の出力が EX-OR ゲート 132 に送られる。また、EX-OR ゲート 132 には、ブロックデータ D_0 以外のデータとの間の関数 $f(D_i)$ が送られる。

【0115】EX-OR ゲート 132 で、ブロック暗号復号回路 131 の出力と、ブロックデータ D_j 以外のデータとの関数 $f(D_i)$ との EX-OR がとられて、ブロックデータ D_0 が復号される。

【0116】ブロックデータ D_0 が復号されたら、図 8 に示すように、暗号化ブロックデータ ED_1 と、鍵情報 K とがブロック暗号復号回路 121 に送られ、ブロック暗号復号回路 121 で、暗号の復号処理が行われる。

【0117】ブロック暗号復号回路 121 の出力が EX-OR ゲート 122 に送られる。また、EX-OR ゲート 122 には、初期値 inV が送られる。初期値 inV は、暗号化ブロックデータ ED_0 である。

【0118】EX-OR ゲート 122 で、ブロック暗号復号回路 121 の出力と、暗号化ブロックデータ ED_0 との EX-OR がとられて、ブロックデータ D_1 が復号される。

【0119】次に、暗号化ブロックデータ ED_2 と、鍵情報 K とがブロック暗号復号回路 121 に送られる。ブロック暗号復号回路 121 で暗号復号処理が行われる。

【0120】ブロック暗号復号回路 121 の出力が EX-OR ゲート 122 に送られる。また、EX-OR ゲート 122 には、その前の暗号化ブロックデータ ED_1 が送られる。

【0121】EX-OR ゲート 122 で、ブロック暗号復号回路 121 の出力と、その前の暗号化ブロックデータ ED_1 との EX-OR がとられて、ブロックデータ D_2 が復号される。

【0122】以下、暗号化ブロックデータ ED_{255} が復

号されるまで、同様な処理が繰り返される。

【0123】初期値として使った入力ブロックデータ D_j が最後のブロックデータ ($j=255$) のときには、以下のようにして復号化が行われる。

【0124】まず、図 8 に示すように、暗号化ブロックデータ ED_0 と、鍵情報 K とがブロック暗号復号回路 121 に送られ、ブロック暗号復号回路 121 で、暗号の復号処理が行われる。

【0125】ブロック暗号復号回路 121 の出力が EX-OR ゲート 122 に送られる。また、EX-OR ゲート 122 には、初期値 inV が送られる。この初期値 inV は、暗号化ブロックデータ ED_{255} である。

【0126】EX-OR ゲート 122 で、ブロック暗号復号回路 121 の出力と、暗号化ブロックデータ ED_{255} との EX-OR がとられて、ブロックデータ D_0 が復号される。

【0127】次に、暗号化ブロックデータ ED_1 と、鍵情報 K とがブロック暗号復号回路 121 に送られる。ブロック暗号復号回路 121 で暗号が復号される。ブロック暗号復号回路 121 の出力が EX-OR ゲート 122 に送られる。

【0128】また、EX-OR ゲート 122 には、その前の暗号化ブロックデータ ED_0 が送られる。

【0129】EX-OR ゲート 122 で、ブロック暗号復号回路 121 の出力と、その前の暗号化ブロックデータ ED_0 との EX-OR がとられて、ブロックデータ D_1 が復号される。

【0130】以下、同様に、暗号化ブロックデータ ED_2 、 ED_3 、…から、ブロックデータ D_2 、 D_3 、…が復号されていく。

【0131】暗号化ブロックデータ ED_{254} から、ブロックデータ D_{254} が復号されたら、図 9 に示すように、暗号化ブロックデータ ED_{255} と、鍵情報 K とがブロック暗号復号回路 121 に送られ、ブロック暗号復号回路 131 で暗号の復号処理が行われる。

【0132】ブロック暗号復号回路 131 の出力が EX-OR ゲート 132 に送られる。また、EX-OR ゲート 132 には、ブロックデータ D_j 以外のデータとの間の関数 $f(D_i)$ が送られる。

【0133】EX-OR ゲート 132 で、ブロック暗号復号回路 131 の出力と、ブロックデータ D_j 以外のデータとの間の関数 $f(D_i)$ との EX-OR がとられて、ブロックデータ D_{255} が復号される。

【0134】なお、上述の例では、連鎖も初期値も鍵情報も、全て、64 ビットで処理しているが、128 ビットでも、256 ビットでも良い。

【0135】図 10～図 12 は、上述のように、データを暗号化して記録するときの処理を示すフローチャートである。この処理では、例えば 2048 バイトからなる 1 セクタが CBC により暗号化される。1 セクタは、8

バイト（64ビット）毎の256のブロックに分割される。

【0136】図10において、先ず、1セクタ（例えば2048バイト）に相当するブロックデータD0～D255のうちの1つのブロックデータD_jが読み出される（ステップS1）。そして、ブロックデータD_iの関数f(D_i)とのEX-ORが鍵情報Kにより暗号化されて、初期値i n Vが生成される（ステップS2）。この初期値i n Vが保存される（ステップS3）。

【0137】そして、初期値を作るのに用いたブロックデータD_jが最初のブロックデータ（j=0）か否かが判断される（ステップS4）。 10

【0138】（j=0）なら、初期値i n Vが読み出され（ステップS5）、この初期値i n VがブロックデータD0の暗号化ブロックデータED0とされる（ステップS6）。求められた暗号化ブロックデータED0が保存される（ステップS7）。

【0139】ブロックデータの番号iが（i=1）に初期化される（ステップS8）。初期値i n Vが読み出され（暗号化ブロックデータD0と等しい）（ステップS9）、ブロックデータD1が読み出される（ステップS10）。初期値i n VとブロックデータD1とのEX-ORが鍵情報Kで暗号化され、ブロックデータD1の暗号化ブロックデータED1が生成される（ステップS11）。この暗号化ブロックデータED_iが保存される（ステップS12）。そして、ブロックデータの番号iが（i=2）にインクリメントされる（ステップS13）。 20

【0140】ブロックデータの番号iがインクリメントされたら、暗号化ブロックデータED_{i-1}が読み出され（ステップS14）、ブロックデータD_iが読み出される（ステップS15）。暗号化ブロックデータED_{i-1}とブロックデータD_iとのEX-ORが鍵情報Kで暗号化され、ブロックデータD_iの暗号化ブロックデータED_iが生成される（ステップS16）。この暗号化ブロックデータED_iが保存される（ステップS17）。そして、ブロックデータの番号iがインクリメントされる（ステップS18）。 30

【0141】ブロック番号iが「256」に達したか否かが判断され（ステップS19）、ブロック番号iが「256」に達していなければ、ステップS14にリターンされる。そして、ブロック番号iが「256」に達するまで、同様の処理が繰り返され、暗号化ブロックデータED_iが求められていき、ブロック番号iが「256」に達してブロックデータD255まで求められたら処理が終了される。 40

【0142】ステップS4で、初期値を作るのに用いたブロックデータD_jが最初のブロックデータ（j=0）でなければ、図11に示すように、初期値を作るのに用いたブロックデータD_jが最後のブロックデータ（j= 50

255）か否かが判断される（ステップS20）。

【0143】（j=255）なら、ブロック番号iが（i=0）に初期化される（ステップS21）。そして、ステップS2で求められた初期値i n Vが読み出され（ステップS22）、ブロックデータD0が読み出される（ステップS23）。初期値i n VとブロックデータD0とのEX-ORが鍵情報Kで暗号化され、ブロックデータD0の暗号化ブロックデータED0が生成される（ステップS24）。この暗号化ブロックデータED0が保存される（ステップS25）。そして、ブロックデータの番号iが（i=1）にインクリメントされる（ステップS26）。 10

【0144】ブロックデータの番号iがインクリメントされたら、暗号化ブロックデータED_{i-1}が読み出され（ステップS27）、ブロックデータD_iが読み出される（ステップS28）。暗号化ブロックデータED_{i-1}とブロックデータD_iとのEX-ORが鍵情報Kで暗号化され、ブロックデータD_iの暗号化ブロックデータED_iが生成される（ステップS29）。この暗号化ブロックデータED_iが保存される（ステップS30）。そして、ブロックデータの番号iがインクリメントされる（ステップS31）。 20

【0145】ブロック番号iが「255」に達したか否かが判断され（ステップS32）、ブロック番号iが「255」に達していなければ、ステップS27にリターンされる。そして、ブロック番号iが「255」に達するまで、同様の処理が繰り返され、暗号化ブロックデータED_iが求められていく。

【0146】ブロック番号が「255」になったら、ステップS2で求められた初期値i n Vが読み出される（ステップS33）。そして、この初期値i n Vが暗号化ブロックデータED255とされて（ステップS34）、保存され（ステップS35）、処理が終了される。 30

【0147】ステップS4で初期値を作るのに用いたブロックデータD_jが最初のブロックデータ（j=0）ではないと判断され、ステップS20で、最後のブロックデータ（j=255）でもない判断されたら、図12に示すように、ブロックデータの番号iが（i=0）に初期化される（ステップS36）。ステップS2で求められた初期値i n Vが読み出され（ステップS37）、ブロックデータD0が読み出される（ステップS38）。初期値i n VとブロックデータD0とのEX-ORが鍵情報Kで暗号化され、ブロックデータD0の暗号化ブロックデータED0が生成される（ステップS39）。この暗号化ブロックデータED0が保存される（ステップS40）。そして、ブロックデータの番号iが（i=1）にインクリメントされる（ステップS41）。 40

【0148】ブロックデータの番号iがインクリメント 50

されたら、今回のブロック番号 i は初期値を作るのに用いる所の番号 j ($j = i$) であるか否かが判断される (ステップ S 4 2)。($j = i$) でなければ、暗号化ブロックデータ ED_{i-1} が読み出され (ステップ S 4 3)、ブロックデータ D_i が読み出される (ステップ S 4 4)。暗号化ブロックデータ ED_{i-1} とブロックデータ D_i との EX-OR が鍵情報 K で暗号化され、ブロックデータ D_i の暗号化ブロックデータ ED_i が生成される (ステップ S 4 5)。この暗号化ブロックデータ ED_i が保存される (ステップ S 4 6)。そして、ブロックデータの番号 i がインクリメントされる (ステップ S 4 7)。

【0149】ブロック番号 i が「256」に達したか否かが判断され (ステップ S 4 8)、ブロック番号 i が「256」に達していなければ、ステップ S 4 2 にリターンされる。

【0150】ステップ S 4 2 で、($j = i$) であると判断されたら、ステップ S 2 で求められた初期値 inV が読み出され (ステップ S 4 9)、この初期値 inV がブロックデータ D_j の暗号化ブロックデータ ED_j とされる (ステップ S 5 0)。この暗号化ブロックデータ ED_j が保存される (ステップ S 5 1)。そして、ステップ S 4 7 に進む。

【0151】そして、ブロック番号 i が「256」に達するまで、同様の処理が繰り返される。ブロック番号 i が「256」に達し、ブロックデータ D_{255} までの暗号化ブロックデータが求められたら、処理が終了される。

【0152】次に、暗号を復号するときの処理について説明する。図 13～図 16 は、暗号を復号する場合の処理を示すフローチャートである。

【0153】図 13～図 16 において、初期値として用いたブロック番号 j が ($j = 0$) か否かが判断される (ステップ S 1 0 1)。

【0154】($j = 0$) のときには、暗号化ブロックデータ ED_0 が読み出される (ステップ S 1 0 2)。この暗号化ブロックデータ ED_0 が鍵情報 K で復号され、この復号値と関数 $f(D_i)$ との EX-OR により、ブロックデータ D_0 が生成される (ステップ S 1 0 3)。このブロックデータ D_0 が保存される (ステップ S 1 0 4)。

【0155】ブロック番号 i が ($i = 1$) に初期化される (ステップ S 1 0 5)。暗号化ブロックデータ ED_1 が読み出される (ステップ S 1 0 6)。そして、暗号化ブロックデータ ED_0 が読み出される (ステップ S 1 0 7)。暗号化ブロックデータ ED_0 が初期値 inV とされる (ステップ S 1 0 8)。

【0156】暗号化ブロックデータ ED_1 が鍵情報 K で復号され、この復号値と初期値 inV (暗号化ブロックデータ ED_0 と等しい) との EX-OR がとられて、ブロックデータ D_1 が生成される (ステップ S 1 0 9)。

生成されたブロックデータ D_1 が保存される (ステップ S 1 1 0)。そして、ブロック番号 i が ($i = 2$) にインクリメントされる (ステップ S 1 1 1)。

【0157】暗号化ブロックデータ ED_i が読み出される (ステップ S 1 1 2)。暗号化ブロックデータ ED_{i-1} が読み出される (ステップ S 1 1 3)。暗号化ブロックデータ ED_i が鍵情報 K で復号され、この復号値と暗号化ブロックデータ ED_{i-1} との EX-OR がとられて、ブロックデータ D_i が生成される (ステップ S 1 1 4)。このブロックデータ D_i が保存される (ステップ S 1 1 5)。そして、ブロック番号 i がインクリメントされる (ステップ S 1 1 6)。

【0158】ブロック番号 i が「256」に達したか否かが判断され (ステップ S 1 1 7)、ブロック番号 i が「256」に達していなければ、ステップ S 1 1 2 にリターンされる。ブロック番号 i が「256」に達するまで、同様の処理が繰り返される。ブロック番号 i が「256」に達し、ブロックデータ D_{255} まで復号されたら、処理が終了される。

【0159】ステップ S 1 0 1 で、初期値として用いたブロック番号 j が ($j = 0$) ではないと判断されたら、図 14 に示すように、初期値として用いたブロック番号 j が ($j = 255$) か否かが判断される (ステップ S 1 1 8)。

【0160】($j = 255$) なら、ブロック番号 i が ($i = 0$) に初期化される (ステップ S 1 1 9)。暗号化ブロックデータ ED_0 が読み出される (ステップ S 1 2 0)。暗号化ブロックデータ ED_{255} が読み出される (ステップ S 1 2 1)。暗号化ブロックデータ ED_{255} が初期値 inV とされる (ステップ S 1 2 2)。

【0161】暗号化ブロックデータ ED_0 が鍵情報 K で復号され、この復号値と初期値 inV との EX-OR がとられて、ブロックデータ D_0 が生成される (ステップ S 1 2 3)。生成されたブロックデータ D_0 が保存される (ステップ S 1 2 4)。そして、ブロック番号 i が ($i = 1$) にインクリメントされる (ステップ S 1 2 5)。

【0162】暗号化ブロックデータ ED_i が読み出される (ステップ S 1 2 6)。暗号化ブロックデータ ED_{i-1} が読み出される (ステップ S 1 2 7)。暗号化ブロックデータ ED_i が鍵情報 K で復号され、この復号値と暗号化ブロックデータ ED_{i-1} との EX-OR がとられて、ブロックデータ D_i が生成される (ステップ S 1 2 8)。このブロックデータ D_i が保存される (ステップ S 1 2 9)。そして、ブロック番号 i がインクリメントされる (ステップ S 1 3 0)。

【0163】ブロック番号 i が「255」に達したか否かが判断され (ステップ S 1 3 1)、ブロック番号 i が「255」に達していなければ、ステップ S 1 2 6 にリターンされる。ブロック番号 i が「255」に達するま

で、同様の処理が繰り返される。

【0164】ブロック番号 i が「255」に達し、ブロックデータD254までの処理が完了したら、暗号化ブロックデータED255が読み出される（ステップS132）。この暗号化ブロックデータED255が鍵情報Kで復号され、この復号値と関数 $f(D_i)$ とのEX-ORにより、ブロックデータD255が生成される（ステップS133）。このブロックデータD255が保存されて（ステップS134）、処理が終了される。

【0165】ステップS101で、 $(j=0)$ ではないと判断され、ステップS118で、 $(j=255)$ ではないと判断されたら、図15に示すように、ブロック番号 i が $(i=0)$ に初期化される（ステップS135）。

【0166】暗号化ブロックデータED0が読み出される（ステップS136）。暗号化ブロックデータED j が読み出される（ステップS137）。暗号化ブロックデータED j が初期値 inV とされる（ステップS138）。

【0167】暗号化ブロックデータED0が鍵情報Kで復号され、この復号値と初期値 inV とのEX-ORがとられて、ブロックデータD0が生成される（ステップS139）。生成されたブロックデータD0が保存される（ステップS140）。そして、図16に示すように、ブロック番号 i が $(i=1)$ にインクリメントされる（ステップS141）。

【0168】ブロックデータの番号 i がインクリメントされたら、今回のブロック番号 i は初期値を作るのに用いる所の番号 j ($j=i$) であるか否かが判断される（ステップS142）。

【0169】 $(j=i)$ でなければ、暗号化ブロックデータED i が読み出される（ステップS143）。暗号化ブロックデータED $i-1$ が読み出される（ステップS144）。暗号化ブロックデータED i が鍵情報Kで復号され、この復号値と暗号化ブロックデータED $i-1$ とのEX-ORがとられて、ブロックデータD i が生成される（ステップS145）。このブロックデータD i が保存される（ステップS146）。そして、ブロック番号 i がインクリメントされる（ステップS147）。

【0170】ブロック番号 i が「256」に達したか否かが判断され（ステップS148）、ブロック番号 i が「256」に達していなければ、ステップS142にリターンされる。

【0171】ステップS142で、 $(i=j)$ であると判断されたら、暗号化ブロックデータED j が読み出される（ステップS149）。この暗号化ブロックデータED j が鍵情報Kで復号され、この復号値と関数 $f(D_i)$ とのEX-ORにより、ブロックデータD j が生成される（ステップS150）。このブロックデータD j が保存される（ステップS151）。そして、ステップ

S147に進められる。

【0172】そして、ブロック番号 i が「256」に達するまで、同様の処理が繰り返される。ブロック番号 i が「256」に達し、ブロックデータD255までの復号が完了したら、処理が終了される。

【0173】なお、初期値を暗号化したブロックデータD j については、常に固定の所にしておいても良いし、変更できるようにしても良い。初期値を暗号化したブロックデータD j を変更可能としておくことで、秘匿性を上げることができる。

【0174】以上のように、この発明では、ブロック暗号化を連鎖的に行う場合の初期値を、コンテンツデータそのものから生成している。このため、データ領域のロスがないと共に、コンテンツデータはランダムに変化しているため、秘匿性が高い。

【0175】つまり、コンテンツデータが音楽データのような場合には、サンプリングにより得られたデータであるため、それ自身、ランダム化されたデータであると言える。ある時点の音楽データの値がどのレベルであるかを知ることは、非常に困難なことである。したがって、コンテンツデータ自身から初期値を作ると、乱数を初期値として用いたと同じように、秘匿性が向上する。

【0176】次に、コンテンツのデータとして、MPEGストリームを記録する場合について説明する。

【0177】図1に示したように、CD2の光ディスクは、内周側の領域AR1と、外周側の領域AR2とがあり、領域AR2には、MP3方式でファイル化されたオーディオデータが記録される。MP3方式は、MPEG1で使用されるオーディオデータの3つのレイヤのうちの一つである。したがって、外周側の領域AR2にMP3のデータを記録する場合には、MPEGストリームに準拠して、データの記録が行われる。

【0178】MPEGのストリームは、上位レイヤ（プログラムレイヤ、パッケレイヤ）と、下位レイヤ（パケットレイヤ）でストリームが構成される。すなわち、MPEGストリームでは、1つのプログラムのシーケンスは複数のパックからなり、各パックは、一般的には、複数のパケットから構成される。各パックの先頭には、パケットヘッダが設けられる。パケットは、パケットヘッダとデータとからなる。

【0179】CDでは、98フレームからなるブロックがセクタとされ、このセクタを単位として、データが記録される。

【0180】図17は、CDにMPEGストリームを記録したときのデータ構造を示すものである。図17に示すように、CDの1セクタには、2048バイトのデータ領域が設けられる。この2048バイトのデータ領域に、原則として、1セクタに、MPEGストリームのパック及びパケットが配置される。図18に示すように、

ファイルの先頭には、ファイルヘッダが設けられる。このファイルヘッダには、著作者の管理情報が配置される。

【0181】図17に示すように、1セクタの先頭には、バックヘッダが設けられる。このバックヘッダは、例えば14バイトからなる。このバックヘッダには、バックスタートコードや、SCR (System Clock Reference)、ビットレートが含まれている。

【0182】バックヘッダに続いて、パケットヘッダが設けられる。このパケットヘッダは、例えば、18バ

イトからなる。このパケットヘッダには、パケットスタートコード、ストリームID、PES (Packetized Elementary Stream) ヘッダ長、PTS (Presentation Time Stamp) が含まれている。

【0183】1セクタの残りの2016バイトに、MP EG方式で圧縮されたコンテンツのデータ (例えば、圧縮されたオーディオデータ) が配置される。

【0184】このように、MP3のようなMPEGのファイルは、バックとパケットからなる構成のストリームに組み込まれる。そして、図18に示すように、ファイル

の先頭には、ファイルヘッダが設けられる。このファイルヘッダには、ファイルIDやISRC (International Standard Recording Code) のような著作者の管理情報が含まれる。ISRCは、その曲のマスターテープや作成時に付けられる曲、会社、録音年、レコーディング番号等からなる12桁のコードである。さらに、ディスクを自体を識別できるようなディスクIDを設けるようにしても良い。

【0185】このように、CDにMPEGのストリー

ムを記録する場合には、2048バイトの1セクタのデータ領域に、原則として、バック及びセクタのデータが記録される。これら1セクタのデータのうち暗号化が必要なのは2016バイトのデータであり、14バイトのバックヘッダ及び18バイトのパケットヘッダは暗号化は不要である。

【0186】図19は、1セクタ分のMPEGストリームのコンテンツのデータを暗号化する場合のブロックの構成を示すものである。上述のように、MPEGストリームの場合には、1セクタのデータのうち、暗号化する必要のあるのは、2016バイトのデータである。したがって、MPEGストリームを暗号化する場合には、図19に示すように、1セクタのデータは、8バイト (64ビット) 単位で、252のブロックに分割される。そして、前述と同様に、今回のブロックデータと、その1つ前のブロックデータを暗号化したデータとのEX-ORをとって、暗号化するようなCBC方式により、暗号化される。

【0187】CBC方式で暗号化する場合には、初期値が必要である。前述の例では、初期値を、同一セクタ内のブロックのコンテンツデータから生成するよう

いる。MPEGストリームの場合にも、これと同様に、同一セクタ内のブロックのコンテンツデータそのものから初期値を作っても良いが、MPEGストリームのヘッダのユニーク性を着目して、MPEGストリームのヘッダからCBCの初期値を作るようにしても良い。

【0188】つまり、図17に示したように、MPEGストリームには、バックヘッダと、パケットヘッダとが設けられている。また、図18に示すように、ファイルの先頭には、ファイルヘッダが設けられる。これらのヘッダから初期値を生成することが考えられる。

【0189】例えば、ファイルヘッダには、ISRCのような著作権の管理情報等が記録されている。この著作権の管理情報は、コンテンツ毎にユニークな値である。また、ディスクヘッダがある場合は、ディスクのシリアル番号のように、ディスク毎にユニークな値をディスクヘッダに入れることができる。このような情報は、ディスク毎にユニークな情報である。

【0190】また、バックヘッダは、バックスタートコードや、SCR、ビットレートが含まれている。この中で、SCRは、システムの基準となるSTC (System TimeClock) を較正するための時間情報である。また、パケットヘッダには、パケットスタートコード、ストリームID、PESヘッダ長、PTSが含まれている。この中で、PTSは再生の基準となる時間情報である。バックヘッダのSCRや、パケットヘッダの中のPTSは、時間と共に変化するため、ユニークな値となる。

【0191】このような、MPEGストリームのヘッダに含まれているユニークな情報を使って、CBC方式で暗号化する場合の初期値を生成することができる。

【0192】MPEGストリームのヘッダの中でユニークな情報を使って、CBC方式の初期を生成する場合に、ヘッダの情報をそのまま用いても良いが、ヘッダの情報をそのまま用いると、秘匿性が十分でない。

【0193】そこで、いくつかのMPEGストリームのヘッダの情報から初期値を生成したり、ヘッダの情報を暗号化して、初期値を生成することが考えられる。具体的には、以下の方法が考えられる。

【0194】まず、著作権情報のようなファイルヘッダのユニークな情報と、バックヘッダのSCRやパケットヘッダの中のPTSのような時間と共に変化する情報とを所定の関数により組み合わせる初期値を生成することが考えられる。

【0195】図20は、このように、著作権情報のようなファイルヘッダのユニークな情報と、バックヘッダのSCRやパケットヘッダの中のPTSのような時間と共に変化する情報とから初期値を生成する場合のプロセスの一例である。図20において、EX-ORゲート201には、ファイルヘッダのユニークな情報が供給されると共に、バックヘッダのSCR又はパケットヘッダの中のPTSが供給される。EX-ORゲート201で、フ

10

20

30

40

50

ファイルヘッダのユニークな情報と、パックヘッダのSCR又はパケットヘッダの中のPTSとのEX-ORが求められる。このEX-ORゲート201の出力から、初期値inVが求められる。

【0196】次に、著作権情報のようなファイルヘッダのユニークな情報、又は、パックヘッダのSCRやパケットヘッダの中のPTSのような時間と共に変化する情報を暗号化して、初期値を生成することが考えられる。

【0197】図21Aは、著作権情報のようなファイルヘッダのユニークな情報を暗号化して初期値を生成する場合のプロセスの一例である。図21Aにおいて、暗号化回路211には、ファイルヘッダのユニークな情報が供給される。暗号化回路211で、このファイルヘッダのユニークな情報が暗号化され、暗号化回路211の出力から、初期値inVが求められる。

【0198】図21Bは、パックヘッダのSCRやパケットヘッダの中のPTSのような時間と共に変化する情報を暗号化して初期値を生成する場合のプロセスの一例である。図21Bにおいて、暗号化回路221には、パックヘッダのSCR又はパケットヘッダの中のPTSが供給される。暗号化回路221で、SCR又はPTSが暗号化され、暗号化回路221の出力から、初期値inVが求められる。

【0199】さらに、著作権情報のようなファイルヘッダのユニークな情報と、パックヘッダのSCRやパケットヘッダの中のPTSのような時間と共に変化する情報とから求められる情報を暗号化して、初期値を生成することが考えられる。

【0200】図22は、著作権情報のようなファイルヘッダのユニークな情報と、パックヘッダのSCRやパケットヘッダの中のPTSのような時間と共に変化する情報を、更に、暗号化して、初期値を生成する場合のプロセスの一例である。図22において、EX-ORゲート231には、ファイルヘッダのユニークな情報が供給されると共に、パックヘッダのSCR又はパケットヘッダの中のPTSが供給される。EX-ORゲート231で、ファイルヘッダのユニークな情報と、パックヘッダのSCR又はパケットヘッダの中のPTSとのEX-ORが求められる。このEX-ORゲート231の出力が暗号化回路232に供給される。暗号化回路232で、EX-ORゲート231の出力が暗号化され、暗号化回路232の出力から、初期値inVが求められる。

【0201】図23は、MPEGストリームを暗号化する場合の暗号化プロセスの一例である。図23において、EX-ORゲート301-0で、入力ブロックデータD0と、MPEGヘッダから求められた初期値inVとのEX-ORがとられ、このEX-ORゲート301-0の出力がブロック暗号化回路302-0に供給される。

【0202】ブロック暗号化回路302-0で、EX-

ORゲート311の出力と鍵情報Kとから、暗号化ブロックデータED0が求められる。

【0203】次に、EX-ORゲート301-1で、入力ブロックデータD1と、暗号化ブロックデータED0とのEX-ORがとられ、このEX-ORゲート301-1の出力がブロック暗号化回路302-1に供給され、ブロック暗号化回路302-1で、EX-ORゲート301-1の出力と鍵情報Kとから、暗号化ブロックデータED1が求められる。

【0204】以下、同様にして、入力データD2、D3、…、D251から、暗号化ブロックデータED2、ED3、…、ED251が求められる。

【0205】図24は、MPEGストリームを復号する場合の復号化プロセスの一例である。図24において、暗号化ブロックデータED0と、鍵情報Kとがブロック暗号復号回路401-0に送られ、ブロック暗号復号回路401-0で、暗号の復号処理が行われる。

【0206】ブロック暗号復号回路401-0の出力がEX-ORゲート402-0に送られる。また、EX-ORゲート402-0には、初期値inVが送られる。この初期値inVは、暗号化ブロックデータinVである。

【0207】EX-ORゲート402-0で、ブロック暗号復号回路401-0の出力と、初期値inVとのEX-ORがとられて、ブロックデータD0が復号される。

【0208】次に、暗号化ブロックデータED1と、鍵情報Kとがブロック暗号復号回路401-1に送られる。ブロック暗号復号回路401-1で暗号が復号される。ブロック暗号復号回路401-1の出力がEX-ORゲート402-1に送られる。

【0209】また、EX-ORゲート402-1には、その前の暗号化ブロックデータED0とが送られる。

【0210】EX-ORゲート402-1で、ブロック暗号復号回路401-1の出力と、その前の暗号化ブロックデータED0とのEX-ORがとられて、ブロックデータD1が復号される。

【0211】以下、同様にして、暗号化ブロックデータED1、ED2、…から、ブロックデータD1、D2、…、D251が復号されていく。

【0212】このように、MPEGストリームを記録する場合には、MPEGのヘッダのユニーク性を利用して、MPEGヘッダを使ってCBC方式で暗号化を行う場合の初期値を作ることができる。なお、上述の例では、ファイルヘッダと、パックヘッダ又はパケットヘッダのSCR又はPTS等の時間情報とを使って初期値を生成しているが、さらに、ディスクヘッダの情報をを用いるようにしても良い。

【0213】なお、上述の例では、コンテンツのデータをCD2の光ディスクに記録しているが、記録媒体とし

10

20

30

40

50

ては、CD 2 の光ディスクに限定されるものではない。この発明は、CD-DA や CD-ROM、CD-R や CD-RW にコンテンツのデータを記録する場合にも、同様に適用することができる。また、光ディスクに限らず、磁気ディスク、フラッシュメモ리카ード等、種々の記録媒体にコンテンツのデータを記録する場合に同様に適用できる。

【0214】さらに、この発明は、コンテンツのデータをネットワークで配信する場合に用いても好適である。

【0215】つまり、近年、音楽データのようなコンテンツのデータをネットワークを使って配信するようなサービスが普及している。このようなサービスでは、コンテンツのデータの保護を図るために、コンテンツのデータを暗号化することが望まれる。この発明では、ブロック暗号化を連鎖的に行う場合の初期値を、コンテンツデータそのもの又は MPEG ストリームのデータから生成しているため、コンテンツのデータを配信する場合の暗号化にも好都合である。

【0216】

【発明の効果】この発明によれば、コンテンツのデータがブロック化され、鎖状に連鎖して暗号化される。そして、このときの初期値を、そのセクタのコンテンツデータそのものから生成している。このため、初期値を乱数等で発生する必要がなく、データ領域のロスがない。また、コンテンツデータはランダムに変化しているため、秘匿性が高い。更に、乱数発生器等を容易する必要がなく、回路規模が増大しない。

【0217】また、この発明によれば、コンテンツデータから生成される初期値自体が他のコンテンツデータで暗号化される。更に、初期値として使うコンテンツデータを自由に選ぶことができる。これにより、秘匿性が向上される。

【0218】さらに、この発明によれば、MPEG ストリームを記録する場合には、ヘッダに含まれるユニークな情報を使って、初期値を生成している。ヘッダの情報はユニークであり、SCR や PTS のような時間情報は、時間と共に変化するため、秘匿性が高い。また、MPEG ストリームのヘッダの情報を使って暗号化の初期値を形成しているので、MPEG ストリームを保ったまま、伝送することができる。さらに、乱数発生器等を容易する必要がなく、回路規模が増大しない。

【図面の簡単な説明】

【図 1】この発明が適用された光ディスクの一例の略線図である。

【図 2】この発明が適用された記録装置の一例のブロック図である。

【図 3】この発明が適用された再生装置の一例のブロック図である。

【図 4】セクタの構成を示す略線図である。

【図 5】ブロックの構成を示す略線図である。

【図 6】この発明が適用された暗号化処理の説明に用いるブロック図である。

【図 7】この発明が適用された暗号化処理の説明に用いるブロック図である。

【図 8】この発明が適用された復号化処理の説明に用いるブロック図である。

【図 9】この発明が適用された復号化処理の説明に用いるブロック図である。

【図 10】この発明が適用された暗号化処理の説明に用いるフローチャートである。

【図 11】この発明が適用された暗号化処理の説明に用いるフローチャートである。

【図 12】この発明が適用された暗号化処理の説明に用いるフローチャートである。

【図 13】この発明が適用された暗号化処理の説明に用いるフローチャートである。

【図 14】この発明が適用された復号化処理の説明に用いるフローチャートである。

【図 15】この発明が適用された復号化処理の説明に用いるフローチャートである。

【図 16】この発明が適用された復号化処理の説明に用いるフローチャートである。

【図 17】MPEG ストリームを記録する場合の説明に用いる略線図である。

【図 18】MPEG ストリームを記録する場合の説明に用いる略線図である。

【図 19】MPEG ストリームを記録する場合のブロックの構成を示す略線図である。

【図 20】この発明が適用された暗号化処理の説明に用いるブロック図である。

【図 21】この発明が適用された暗号化処理の説明に用いるブロック図である。

【図 22】この発明が適用された暗号化処理の説明に用いるブロック図である。

【図 23】この発明が適用された暗号化処理の説明に用いるブロック図である。

【図 24】この発明が適用された復号化処理の説明に用いるブロック図である。

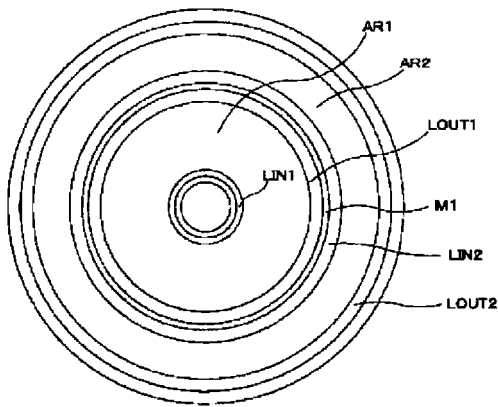
【図 25】従来の暗号化処理の説明に用いるブロック図である。

【図 26】従来の暗号化処理の説明に用いるブロック図である。

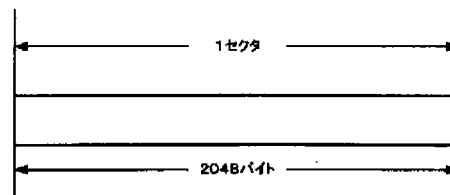
【符号の説明】

4・・・暗号化回路、26・・・暗号解読回路、10、20・・・光ディスク

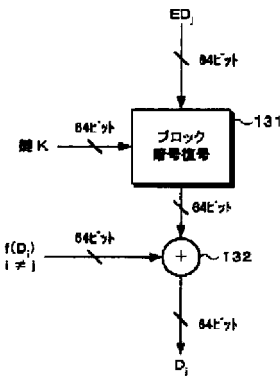
【図 1】



【図 4】



【図 9】

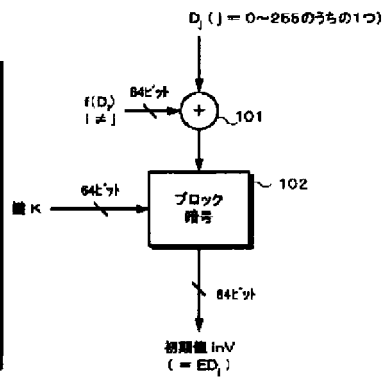


【図 5】

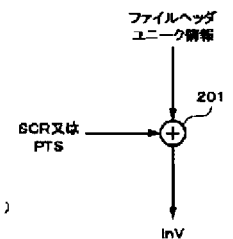
8バイト (84ビット)				
D0	D1	D2	D15
D16	D17	D18	D31
D32	D33	D34	D47
⋮	⋮	⋮	⋮
D240	D241	D242	D255

8バイト × 256 = 2048バイト

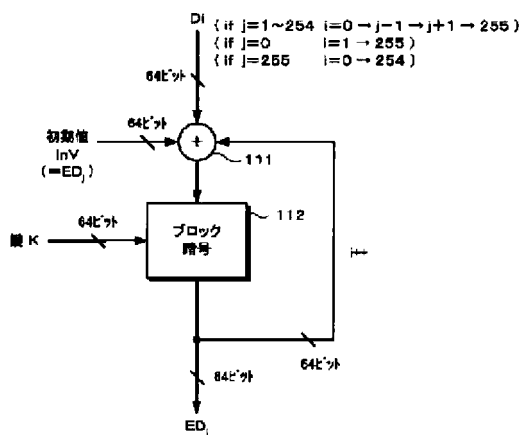
【図 6】



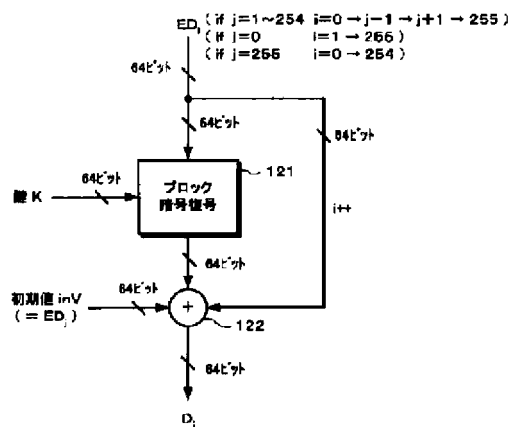
【図 20】



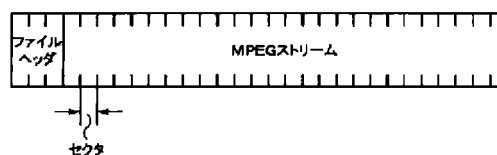
【図 7】



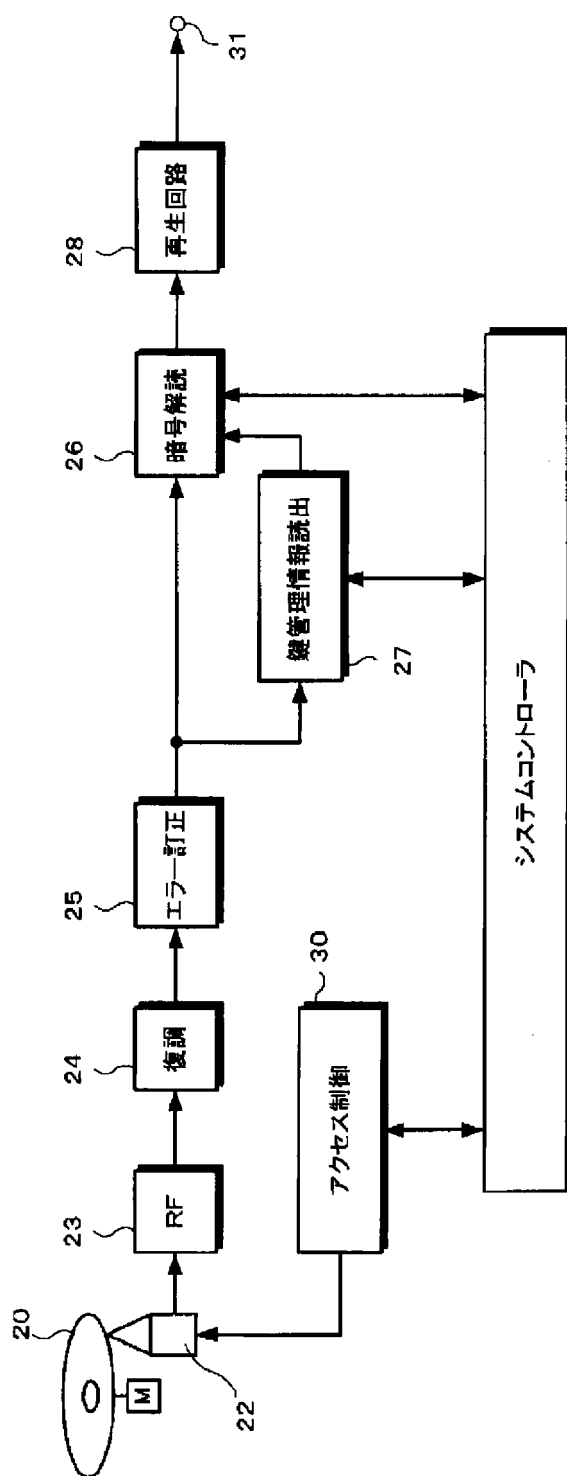
【図 8】



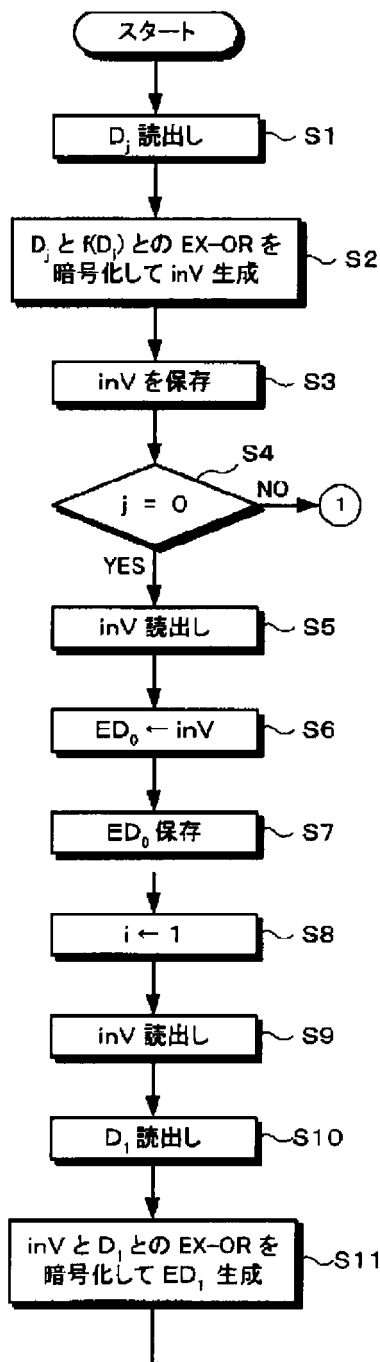
【図 18】



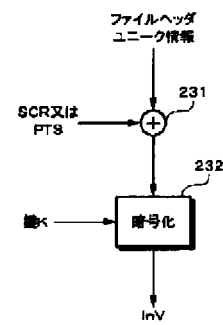
【図 3】



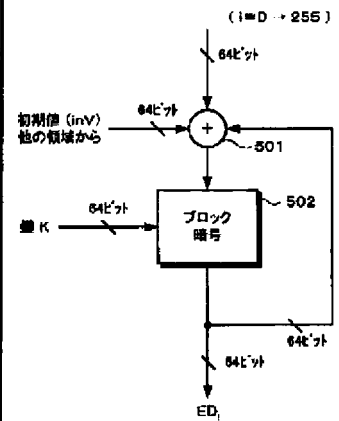
【図10】



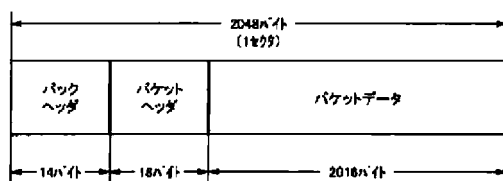
【図22】



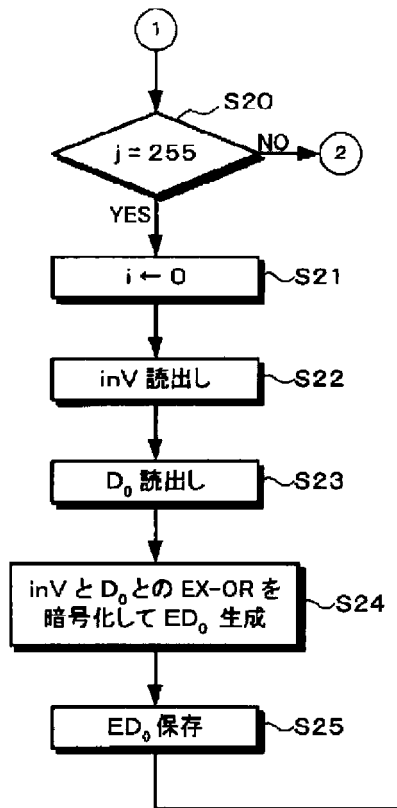
【図25】



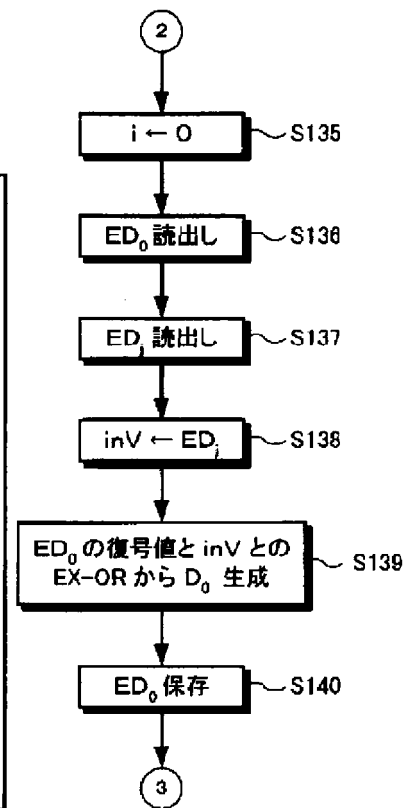
【図17】



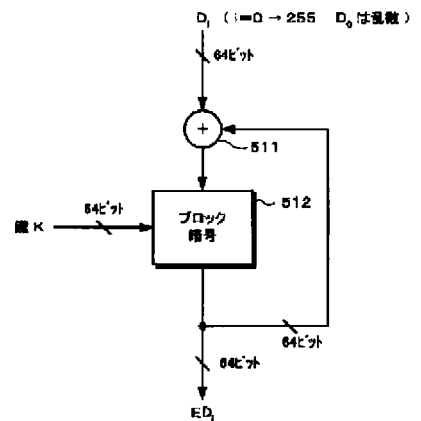
【図 11】



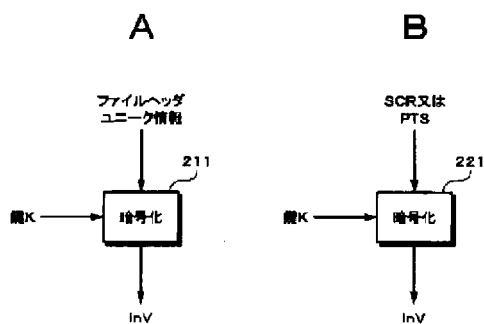
【図 15】



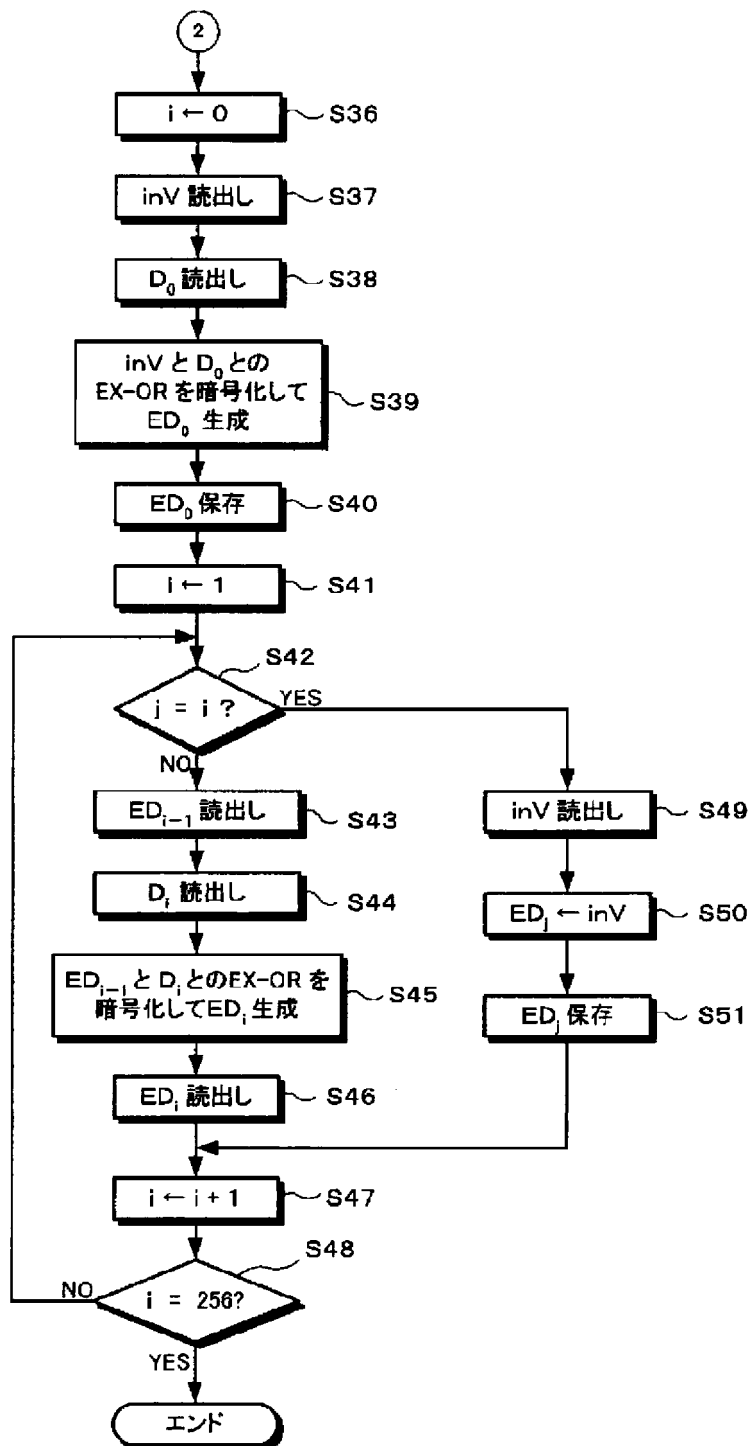
【図 26】



【図 21】



【図12】

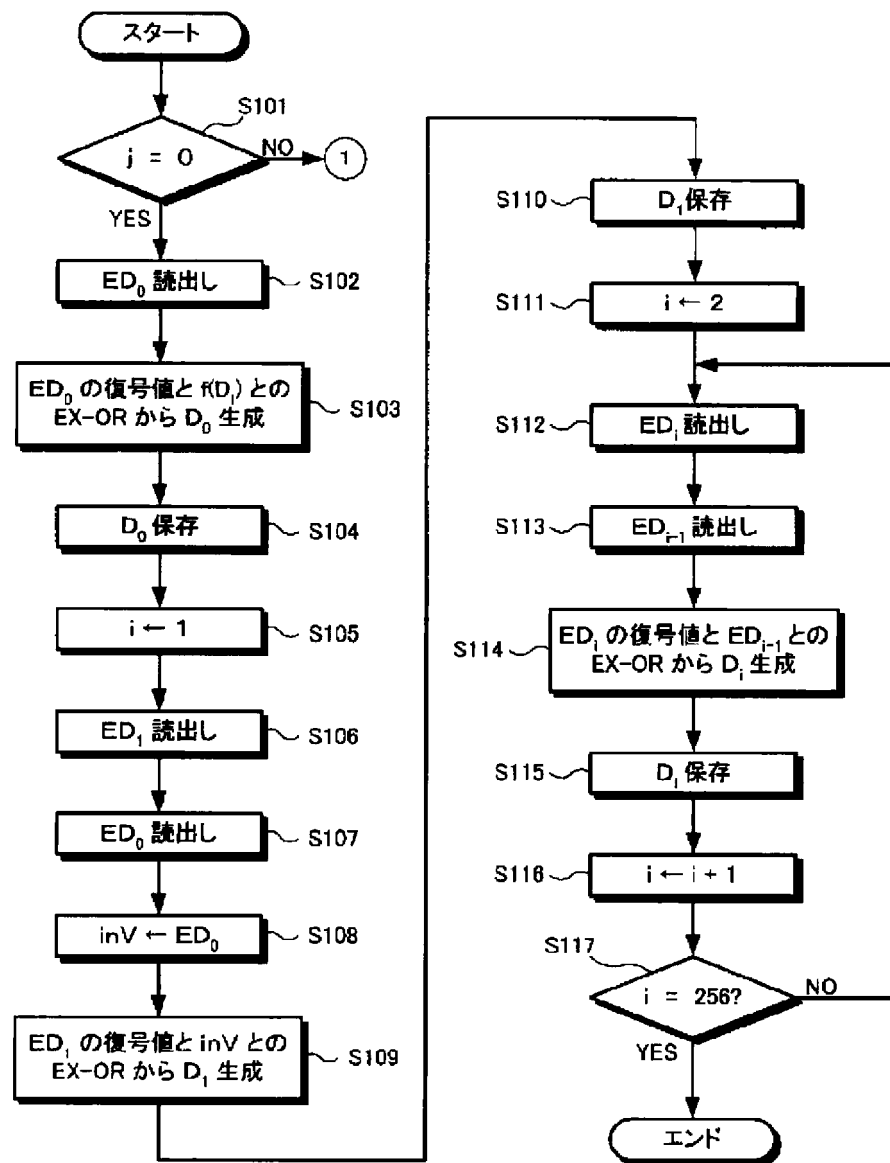


【図19】

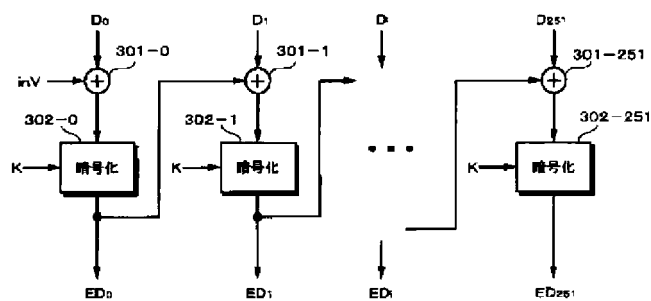
8バイト (64ビット)				
D0	D1	D2	D15
D16	D17	D18	D31
D32	D33	D34	D47
⋮	⋮	⋮	⋮
D240	D241	D242	D251

8バイト × 252 = 2016バイト

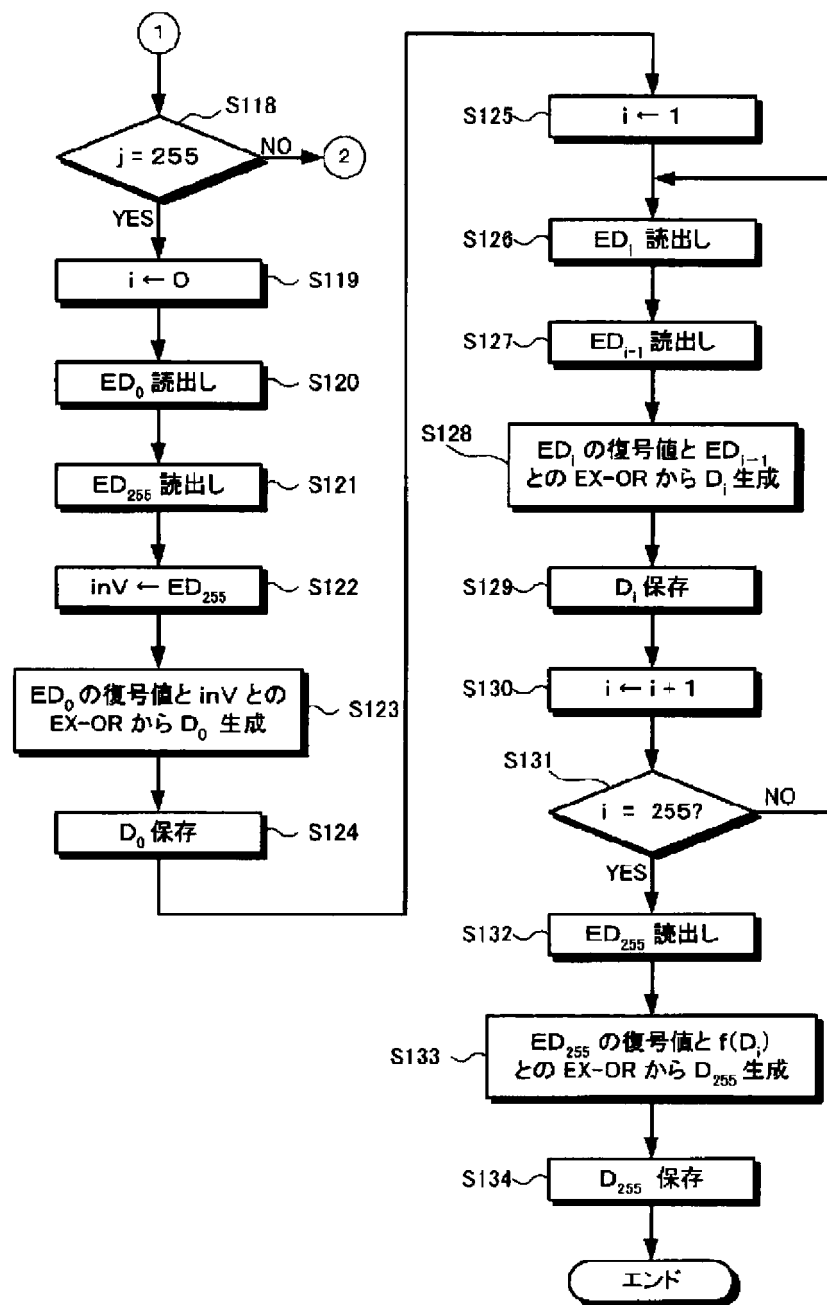
【図13】



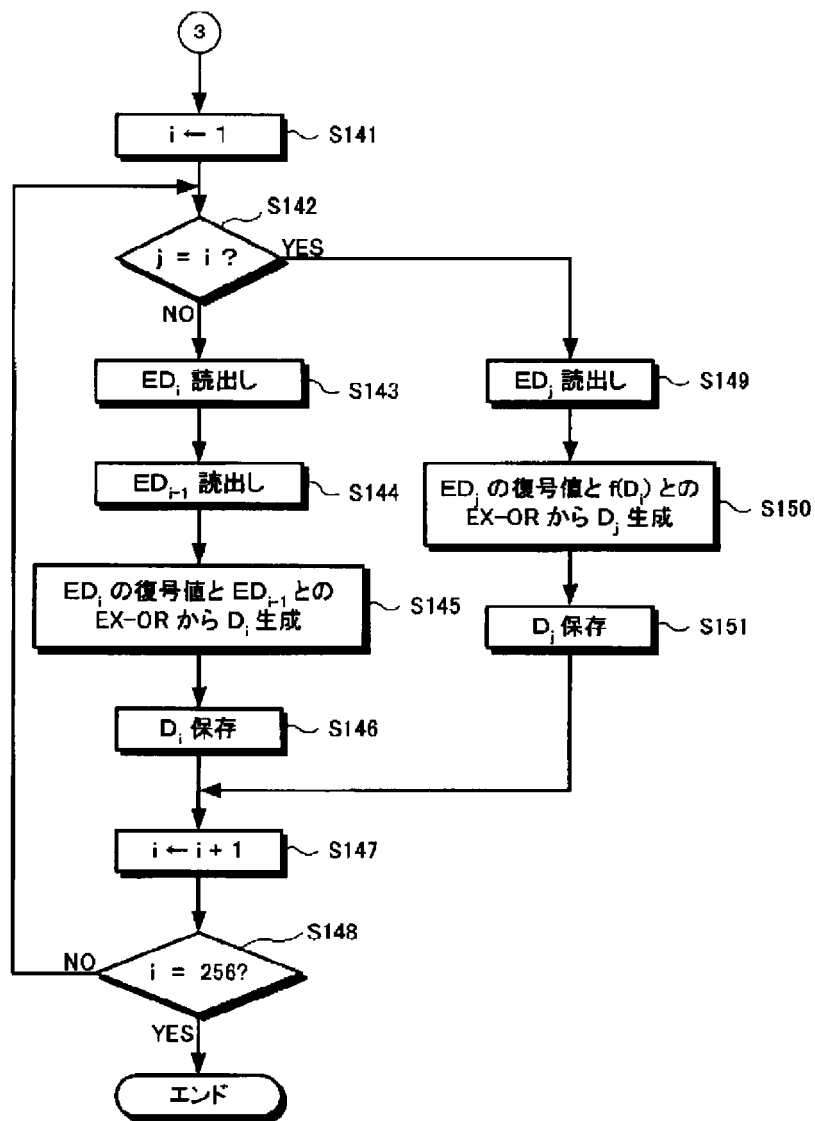
【図23】



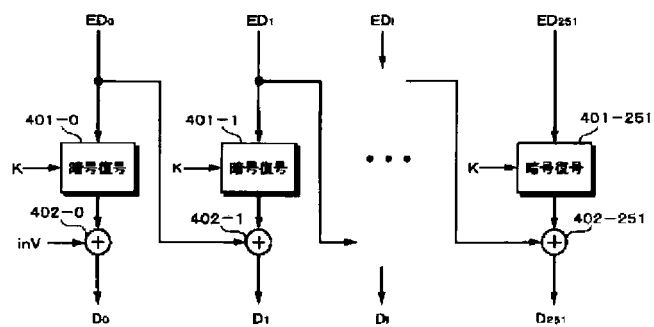
【図 14】



【図 16】



【図 24】



フロントページの続き

(72)発明者 猪口 達也
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(72)発明者 木原 隆
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

Fターム(参考) 5B017 AA03 AA06 AA07 BA07 CA09
CA16
5J104 JA13 NA02